REFERENCE COPY

PENTAGON
MAR 22 1984

# military intelligence

OCT-DEC 1981



counterintelligence

north and south Korean OB

**United States Army Intelligence Center and School**

# Military Intelligence

**BG Richard W. Wilmot**
Commander/Commandant
Autovon 879-2223

**COL Douglas A. Ruane**
Deputy Commander
Autovon 879-2911/2223

**COL Glenn F. Hargis**
Directorate of Combat Developments
Autovon 879-2415/2413

**COL James C. Dottle**
Directorate of Training Developments
Autovon 879-5943/5937

**COL William P. Del Vecchio**
Directorate of Training and Doctrine
Autovon 879-2928/3055

**COL Robert T. Browne**
Directorate of Evaluation
and Standardization
Autovon 879-3405/3518

**COL Michael L. O'Kane**
School Brigade Commander
Autovon 879-2957/2656

**COL Roger L. Dunlap**
US Army Intelligence and
Security Board Commander
Autovon 879-2414

**TRADOC Systems Managers**

**COL Leonard Nowak**
Special Electronic Mission
Aircraft Systems
Autovon 879-5579/5643

**LTC Dean A. Sterling**
Ground Tactical EW/Intel Systems
Autovon 879-5579/5643

**LTC(P) Floyd L. Runyon**
All Source Analysis System
Autovon 879-3504

The United States Army Intelligence Center and School, Fort Huachuca, AZ, is accredited by the North Central Association of Colleges and Schools

## Features

6 **OPSEC in History**
by Captain Michael L. Walsh

12 **Multidiscipline Hostile Intelligence Threat**
by Major Richard L. Felling

18 **North and South Korean OB**
by Thomas A. Marks

25 **I am an All-Source Analyst**
by James C. Mellen

26 **Barcode Labels for Classified Documents**
by James M. Ganz

28 **What's Wrong with "Reliability/Accuracy" Rating Scales**
by Michael G. Samet

35 **Military Currency in International Law**
by Richard A. Banyai

42 **HIND-D Armament: What are the Facts?**
by Donald L. Madill

46 **Geopolitics: The Ultimate in Key Terrain**
by Major Niel E. Nielsen

49 **Mohawks in Hostile Airspace**
by Captain William C. Weaver

53 **Security Education in USAREUR**
by SFC Gary Arrasmith and SSG David Rash

55 **No-Notice Intelligence—82d Style**
by Captain John F. O'Shaughnessy, Jr.

58 **QRT-Dora: Epitaph for a Spy**
by Colonel Richard S. Friedman

MILITARY INTELLIGENCE.
OCT 1981
V.7 I.4 C.1

# School
# Fort Devens

## October—December 1981

## Departments

2 **From the Commander**
3 **Feedback**
4 **Authors**
16 **ACSI Viewpoint**
33 **USAICS/USAISD Notes**
39 **Officers Notes**
40 **Enlisted Notes**
45 **Specialty Proponancy Advocate**

**COL Joseph F. Short**
Deputy Commandant
Autovon 256-2806

**COL R. T. Smith**
School Brigade Commander
Autovon 256-2502

**CSM Roland Van Dyne**
Command Sergeant Major
Autovon 256-2830

**COL Owen H. Knox**
Directorate of Training Developments
Autovon 256-2514

**Dr. William R. Tracey**
Directorate of Training and Doctrine
Autovon 256-2718

**Dr. Edward B. Flynn, Jr.**
Directorate of Evaluation
and Standardization
Autovon 256-2643

**Editor:** 1LT Raymond W. Levesque
**Assistant Editors:** Maria Jansson
Richard A. Banyai
**Art Director/Illustrator:** Herb Gilbert
**Associate Editor:** SSG Larry C. Harmon
**Departments Editor:** SP5 Robert A. Kerr
**Cartoonist:** SP4 Kevin A. Parke

**Military Intelligence**
**(USPS 017-030)**

**Vol. 7, No. 4**

Military Intelligence
Box 569
Fort Huachuca, AZ 85613
Telephone:
Autovon: 879-3033
Commercial: (602) 538-3033

Military Intelligence is published quarterly by the US Army Intelligence Center and School under the provisions of Chapter 5 of AR 310-1 as a professional development resource for military and civilian intelligence personnel. Unless otherwise stated, the ideas presented do not represent the official policy or indorsement by any agency of the US Army or Department of Defense. Authors submitting articles for consideration are responsible for informing the staff of Military Intelligence of simultaneous submission and/or acceptance by other publications. Authors are also responsible for clearing their articles prior to submission if appropriate. Use of funds for printing Military Intelligence was approved by Department of the Army in December 1975. Controlled circulation postage paid at Sierra Vista, Arizona. Subscription rates: 1 year—$6.00: foreign rates: 1 year—$8.00.

The United States Army Intelligence School, Fort Devens, MA, is accredited by the New England Association of Schools and Colleges.

# from the commander

## the need for counterintelligence and HUMINT

by Brigadier General Roy M. Strom

In this era of ever expanding technologies which has seen the development of increased automation and sophistication in the Intelligence-Electronic Warfare spectrum, it is often easy to overlook the fundamental and essential roles of Counterintelligence and HUMINT in the intelligence triad. This issue's "Multidiscipline Hostile Intelligence Services Threat," makes me realize how critical it is for us to be capable of protecting our technology from an enemy whose ability in intelligence collection has never been greater. The task of countering this coordinated assault on our defense capabilities falls on all of us, but specifically it rests with that small body of officers, warrants, and NCOs who General Thompson, the former ACSI, termed the "Army Counterintelligence Service."

"Know your enemy" is an axiom whose importance we in the Army accept and appreciate. Equally important, however, is knowing what the enemy knows about us. We must have that knowledge to preclude us from charging ahead with a false sense of security. That knowledge of what the enemy knows or does not know and how he obtains his information gives us an immeasurable edge. The article, "OPSEC Lessons in History," demonstrates the value gained from exploiting the enemy's intelligence collection means to our advantage. When the enemy can never really trust the validity of the information he has, we have begun to sharpen the edge.

Our efforts in the Counterintelligence and HUMINT field have resulted in monumental successes, as well as catastrophic failures. Dr. Samet's article, "What's Wrong with Reliability and Accuracy Rating Scales?" demonstrates that the HUMINT discipline must also advance, capitalizing on today's technology to insure continued professionalism and prosperity in the only means available to tap into the intentions of the enemy.

It takes but a glance at current newspaper headlines to realize that our open society remains vulnerable to the multidiscipline intelligence collection efforts of our potential adversaries. We have a major challenge today, as in years past, and that is to keep pace with and ferret out those collection activities. Discovery, however, is not enough. As Military Intelligence professionals, we must capitalize on those findings and insure that our commanders are aware of and take action to preclude compromise of our capabilities and intentions. All of us have the responsibility of knowing what operational security is and supporting it in peace as well as in war. Significantly, the Counterintelligence and HUMINT mechanism which contributes to OPSEC does not have to be designed for war and adapted for peacetime operations, as is required for hardware oriented intelligence disciplines and redirection incident to the transition from peace to war. Similarly, the lessons of history drive home the need to maintain a skilled and talented human source collection capability which can augment, reinforce, and trigger our SIGINT and IMINT assets to insure that we "know our enemy."

These are the twin challenges facing Military Intelligence today defensively, to maintain our technological edge and, offensively, to give us a better multidiscipline intelligence collection capability than that directed against us by hostile intelligence services.

# feedback

**Editor:**

Your July-September 1981 edition of Military Intelligence contained a comprehensive article by CPT E.J. Menard on NATO Interoperability at the tactical unit level. CPT Menard highlighted the differences between the US and British staff systems which can and obviously do lead to confusion.

He should perhaps have noted in Figure 4 and the text that in order to achieve complete interoperability within NATO it is necessary for all participants, including the United States and British armies to adopt the NATO General Staff Divisions. It is of course true that the NATO staff nomenclature is modeled after the American system.

CPT Menard will be delighted therefore to hear that effective on 1 Jan 82 the principal divisions of the British Army General Staff are being retitled to bring them into line with the NATO staff divisions:

| NEW DIVISION | OLD DIVISION | PRINCIPAL FUNCTION | SUBSIDIARY FUNCTIONS |
|---|---|---|---|
| G1 | A | Personnel | Manning Discipline Personal Services |
| G2 | G | Intelligence Security | |
| G3 | G | Operations | Staff Duties Exercise Planning Staffs Training Operational Requirements Combat Development Tactical Doctrine |
| G4 | Q | Logistics Including Quartering | |
| G5 | G/Q | Civil/ Military Cooperation | |

Staff appointment titles have been renamed. This should eliminate the confusion that exists when US personnel try to interpret the classic British staff appointment titles. Such an example would be the abbreviated title of "G2 operations" which designates a General Staff Office (GSO) grade 2 (Major) on the Operations Staff. To the American mind, "G2 Ops" is a dichotomy. Accordingly, the appointment titles are being redesignated:

| OLD | NEW |
|---|---|
| Signals | Communications |
| Army Air | Aviation |
| Pay | Finance |
| Electrical and Mechanical Engineers | Maintenance |
| Ordnance | Supply |

The British Ministry of Defense has also directed that the functional titles of certain Arms and Services should be changed:

| RANK/GRADE | OLD | OLD (ABBREVIATED) | NEW |
|---|---|---|---|
| LtCol | GSO1 | G1 | SO1 |
| Major | GSO2 | G2 | SO2 |
| Capt | GSO3 | G3 | SO3 |

I would not presume to occupy any more space in discussing the other Anglo-American problem area raised by CPT Menard—that of language differences. Save to say that, having just arrived as the British Exchange Officer at Fort Huachuca, I had to agree with him!

**R. A. Eccles**
Major
Intelligence Corps

**Editor:**

1 July 1982, marked the nineteenth anniversary of our existence as the Military Intelligence Branch of the United States Army, and needless to say, in such a relatively short time we have achieved tremendous progress and an admirable reputation. For many of us who had grown and marched together with her, the sounds of such a progess can still be heard.

In my personal opinion they represent the glories of past and present sacrifices and could serve as a true source of inspiration and incentive for future ones.

I would like to see in your future issues comments or references about the different activities that took place within the MI communities, worldwide, to commemorate such a magnificent event.

**Juan-Manuel Valera**
CW2, MI
179th MID/197th Inf Bde (SEP)

**Editor:**

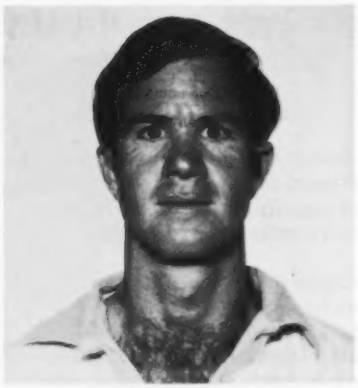
I just received the April-June issue of Military Intelligence. I thought I would write and compliment you on the magazine. Virtually, all the articles were of value and well done. I especially enjoyed the article by Major

**feedback continued on page 61**

# authors

Capt. Michael L. Walsh holds a BS in Law Enforcement from the University of Arizona. He was commissioned through the Reserve Officer Training Corps, and was a distinguished graduate of the program. A 1977 graduate of the MI Officers Basic and Tactical Intelligence Staff Officers Courses, he served three years with the 193d Infantry Brigade in Panama. His assignments there included Platoon Leader with the 193d Military Intelligence Company (CEWI), and S2/HHD Commander, 193d Combat Support Battalion. After attending the MI Officer Advance Course, Walsh is presently the Military Intelligence/Electronic Warfare Assistor, assigned to Readiness Group Meade at Fort George G. Meade, Maryland.

Major Richard L. Felling is a Senior Counterintelligence Analyst with the Counterintelligence Production Division, Intelligence and Threat Analysis Center, United States Army Intelligence and Security Command, Arlington Hall Station, Virginia. He received his Bachelors Degree from Louisiana State University in 1970, and graduated from the Command and General Staff College in 1980. Previous assignments include the 525th MI Group, Vietnam; Battalion S2, 3-60 Infantry; G2 operations, 9th Infantry Division; Group S2, 502d ASA Group; Special Security Officer, Munich, FRG; Company Commander/Headquarters Commandant, 66th MI Group.



Thomas A. Marks graduated from the United States Military Academy in 1972 and served five years on active duty before leaving the service as a Captain in Military Intelligence. He subsequently spent three years as Administrative Assistant to Representative Jack Larsen of the Hawaii State House of Representatives and is now a Ph.D. candidate and Teaching Assistant in Political Science at the University of Hawaii in Honolulu. During the past decade, Mr. Marks has spent considerable time in Asia, publishing numerous articles and monographs on the political and military aspects of the region. His doctoral thesis deals with Thai communism. Marks is currently assigned as the G2 Chemical Officer for IX Corps (USAR). Previously he was the BICC Officer in the 29th Infantry Brigade, Hawaii Army National Guard.

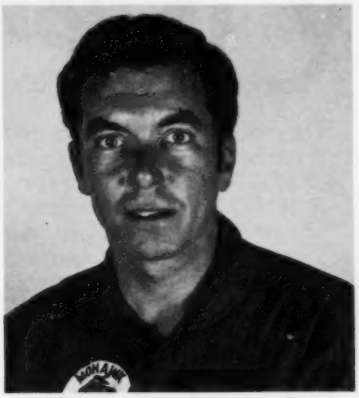
Mr. James C. Mellen is a member of the All-Source Analysis System Support Office at USAICS, where he serves as one of the primary team members documenting the requirements, operational, and organizational plans concerning the ASAS. Mr. Mellen relies on 27 years of experience in MI—a period which includes 11 years in training and training developments, and four years in operational testing and test support of EWI systems. OCONUS tours include Alaska, Pakistan, RVN, Tokyo, and Germany; the latter as the maintenance officer for GUARDRAIL and QUICKLOOK systems.

James M. Ganz is Chief, Administrative Services and Support Division, U.S. Army Signals Warfare Laboratory, Vint Hill Farms Station, Warrenton, Va. He is a graduate of U.S. Army Sergeants Major Academy and received a BA in Business Management from Hampton Institute, and an MBA in General Management from Golden Gate University. Ganz served 20 years active duty with the U.S. Army and retired as command sergeant major with a reserve commission of Captain in the Signal Corps. He has had seven overseas tours that include Germany, Turkey, Taiwan, Thailand, and Vietnam.

Michael G. Samet is Group Director for Command and Control Systems at Perceptronics, Inc. Woodland Hills, Calif. He received his Ph.D. degree in experimental psychology from Tufts University in 1971. His research activities have focused on human information processing, decision making, and the user-computer aspects of interactive systems. From 1973 to 1976, he was a member of the faculty of the Technion—Israel Institute of Technology in Haifa, Israel, where he coordinated research and taught in the departments of Industrial and Management Engineering and Computer Science concerning engineering and systems psychology and human factors in computer systems. Between 1967 and 1973, Samet served as a Senior Research Scientist at the U.S. Army Research Institute for the Behavioral and Social Sciences (Alexandria, VA).

Since 1978, Mr. Donald L. Madill has been an intelligence research specialist in the Threats Directorate, Combined Arms Combat Development Activity, Fort Leavenworth, Kan. Prior to that, he served as a traffic analyst and German linguist in the Army Security Agency in Vietnam and in Germany, where he was commissioned as a signals intelligence officer. He later served in the reserves as a psychological operations officer. He holds a B.S. Ed. degree in German and English from the University of Kansas and a M.A. in foreign languages from Emporia State University. He has studied as a Fulbright scholar at the Friedrich Alexander Universitat in Erlangen, West Germany and is a Ph.D. candidate at the University of Kansas.

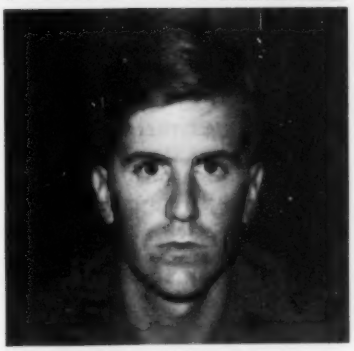
Major Niel E. Nielsen is an instructor at San Jose State University for the 4th ROTC Region. Nielsen holds BA degrees in Criminal Justice and Public Administration from San Jose State University and a Master's in Public Administration from Golden Gate University. A graduate of the Infantry and MI Officers Courses and the Military Police Officers Advanced Course, Nielsen has worked in various MI and MP positions in Vietnam, Korea, Fort Ord and Presidio of San Francisco, Calif.



Capt. Bill Weaver holds a BBA from Loyola University and a MA in Management from Central Michigan University. He is currently the Flight Operations Officer for the 224th MI Bn (AE), Hunter Army Airfield, GA. Weaver's military training include the Infantry Officer Basic School, Airborne School, Civil Affairs School, Rotary Wing, Fixed Wing, OV-1 Flight Training, Tactical Intelligence Staff Officers course and the MI Advanced course. His assignments have included Bn S-2 1/51 INF, 1 AD, Germany; Imagery Sensor Instructor Pilot, USAICS, Fort Huachuca; CDR, Co G, USAICS, Fort Huachuca; USAICS FLT OPNS, Fort Huachuca;Bn S-2 24th AVN Bn, 24th ID, HAAF. Weaver will assume command of A Co (Aerial Surveillance), 224th MI Bn (AE) in January 1982.

SFC Arrasmith is currently NCOIC, Security Branch, CI Division, ODCSI, HQ USAREUR and 7th Army. Previous assignments include Action Officer, Disclosure Office, Office of Chief of Staff, TRADOC, Fort Monroe, Va; NCOIC, Personnel Security Branch, CI Division, ODCSI, HQ USAREUR and 7th Army; and Intelligence Analyst, Airborne Studies Group, HQ MACV (SOG).

SSG Rash is assigned to the Information Security Section, Security Branch, Counterintelligence Division, ODCSI, HQ USAREUR and 7th Army. Previous assignments include BICC NCO, 2/58th Infantry Battalion, 1st Brigade, 2d Armored Division; Security Specialist, 1st Signal Brigade (ACC), Korea; NCOIC Analysis and Production Section, ASIC, 1st Military Intelligence Company, 1st Infantry Division, Fort Riley, Kan.



Captain John F. O'Shaughnessy, Jr. is the BICC officer and assistant S2 of the 1st Brigade, 82d Airborne Division. He holds a BS in Political Science and an MBA from the University of Santa Clara. O'Shaughnessy was the battalion S2 for 2d Battalion (Airborne), 504th Infantry, after attending the MI Officer Basic Course. He is also airborne and jumpmaster qualified.

# OPSEC

Historically, the Soviet Union has placed considerable importance on tactical collection activities, dating back to roving bands of Cossack scouts. Today, Soviet doctrine emphatically calls for fully integrated and continuous combat reconnaissance. Both strategic and tactical Soviet signal intelligence (SIGINT) systems, while foregoing the extreme sophistication of Western design, are still numerous and highly effective. Intelligence-gathering fishing trawlers regularly patrol in or near areas of special Soviet interest.

In addition, NATO forces may face a numerically superior foe in any future conflict. Only by concentrating available forces at key times can NATO possibly hope to overcome this disadvantage. This strategy will require that strict security be maintained before and during all operations. Operations security (OPSEC) therefore must be a combination of all the following elements: deception, information security, signal security (SIGSEC), and physical security.

We can best appreciate the value of proper OPSEC by reviewing battles throughout history which have been won or lost depending on how well informed the enemy was.

### 1780 (Benedict Arnold's Conspiracy)

Disenchanted at having been passed over for promotion, General Benedict Arnold made little secret of his dissatisfaction with the Continental Army. Although an obviously poor security risk, General Arnold was still appointed to command West Point, a strategically important fortress whose loss would split the colonies north and south. Arnold's plot to surrender West Point was uncovered after British Major Andre met with him and, dressed in civilian clothes, was given a safe conduct pass by Arnold to get him through Colonial lines. While heading back to his ship, Andre was confronted by three soldiers in British greatcoats. Relieved at seeing his own countrymen, he disclosed his reason for being there, admitted he was a British officer, and showed them the pass from Arnold as well as a piece of jewelry with his proper name engraved. Andre's disclosure of far more than these soldiers had a "need to know" cost him dearly. The three men were, in fact, Colonials who had somehow appropriated British overcoats for warmth. Major Andre was hanged as a spy, and the British attempt to seize West Point was foiled.

### 1862 (The Battle of Antietam)

The events leading up to the Battle of Antietam on September 13, 1862, are prime examples of what can occur when poor information security is observed. Several days before the battle, the Union Army prepared a camp on the same ground where the Confederate forces had camped just the day before. While rummaging through some of the debris in the area, a Union private found, wrapped around three cigars, a copy of the complete and detailed disposition of the entire Army of Northern Virginia. The paper was transmitted up to General McClellan's staff, and plans were made to punch through the weakest part of the line and envelop the Confederates. Poor security was maintained on the operation, however, and news of the "find" spread throughout the camp. It was picked up by a Confederate agent disguised as a civilian merchant. Forewarned, the Confederates moved up reinforcements to fill the gaps, and managed to withdraw with their forces intact.

# in history

by Captain Michael L. Walsh

### 1918 (The Battle of Megiddo)

In September, 1918, the British under General Allenby were preparing to attack the Turkish forces at Megiddo, north of Palestine. Realizing that any attack would have to be across the Auja River, Allenby planned far enough ahead and established an engineer school on the banks of the river two months before the attack. Consequently, when a variety of new bridges were constructed they did not arouse Turkish suspicion. The attack caught the Turks completely offguard and the Turkish Armies in Syria were destroyed within six weeks.

### 1939-1945 (WORLD WAR II)

The technological leaps in aviation and electronics, as well as the finesse gained by the employment of espionage agents, between the world wars made it much easier to gain intelligence on the enemy. To guard against this, special units such as Britain's London Controlling Staff were created for the sole purpose of strategic deception. Allied and Axis field commanders became cognizant of the importance of tactical deception and the need for tight security surrounding their operations.

This emphasis on security, and the fact that no war in history is so well documented as WW II, makes it possible to find numerous examples of security successes or failures.

### 1939-1943 (The Battle of the Atlantic)

During the period September 1939 to June 1943, German U-Boats sunk 11 million tons of supplies bound for England. This can be attributed both to poor British SIGSEC and the great cryptoanalytic skills of the German Beobactung-Dienst (B-Dienst). Directly answerable to Admiral Doenitz of U-Boat Command, this unit had a vast knowledge of British naval cryptosystems dating back to the Spanish Civil War when the Royal Navy patrolled the European coast to enforce the arms embargo. Despite the outbreak of WW II, the British naval codes were not changed. They continued to use the peacetime systems. As a result, B-Dienst intercepted and read all convoy instructions.

In mid-1941, Britain learned that their code had been compromised and devised a new cipher. This new system had two fatal flaws: 1) It kept the same coded groups for the identification of addressees and originators; and 2) Unlike a one-time pad, it was simply a book, whose pages were used repeatedly. The pages contained columns of random numbers which were added to the coded message to "double encrypt" it. By collecting thousands of messages each month, and through meticulous analysis using the known identification codes, B-Dienst constructed a "shadow book" of their own in February 1942. Using this knowledge they continued to read British naval messages until May 1943, when Britain introduced a newer, more complicated naval code. Loss of this intelligence contributed to the fact that German U-Boats sunk only 3 million tons of supplies the rest of World War II.

### 1939-1945 (Protecting ULTRA)

No less remarkable than the British B-Dienst was the British section at Bletchley, England. With a model of the German encryption machine (Enigma), this section broke the German military code. Realizing its importance, they took strict precautions to avoid compromising what Winston Churchill called, "my most secret source."

Whenever possible, they employed close relatives or long-time friends at the Bletchley intercept site. The British felt that where total security was vital, family ties proved more reliable than detailed screening.

Special Liaison Units (SLU) were devised to insure close control of ULTRA distribution. Liaison personnel were attached to each field commander to insure that the following precautions were taken in handling the information: SLU men personally delivered ULTRA intercepts to authorized commanders; all messages were returned to the SLU men after being read and understood by the recipient; and, perhaps the most critical requirement, no action could be taken which did not include a cover action to explain to the Germans how the Allies might have reached their decision.

The tight information security maintained on ULTRA material enabled the Allies to keep this important source open throughout the war.

### 1942 (Deception at El Alamein)

When the German offensive in North Africa bogged down due to shortage of fuel and supplies, General Montgomery was directed to go on the offensive. As described by Montgomery's Chief of Staff, he was to "hide 160,000 men on a plain as flat and barren as a billiards table, and while the enemy is watching you he must never know what you are doing."[1]

Montgomery did just that; concealing as long as possible his intent to take the initiative and, when this could no longer be done, misleading the Germans as to the place of the attack. Operation BERTRAM, as

the overall deception plan was code named, consisted of two major parts: 1) Gathering supplies and equipment in the north near El Alamein, and 2) Giving the appearance of a planned attack 30 to 50 kilometers south of the actual site.

Some of the steps taken to conceal the build-up in the north included:
1) Hiding boxes of supplies within a network of trenches, thus eliminating telltale shadows from German aerial photos.
2) Disguising the equipment as something less suspicious, then inviting attention to it. For example, boxes were stacked in the shape of a truck and covered with a camouflage net.
3) Gradually extending known ammo dumps, night after night, so that the enlargement wouldn't be noticed.

The decoys in the south sector included:
1) Constructing a dummy pipeline, supposedly to carry water to troops concentrated in the south.
2) Three weeks before the attack, concentrating 4,000 tanks and vehicles in an assembly area 55 kilometers from El Alamein to accustom the enemy to seeing a mass of armor and transports. On October 21 and 22, they moved the genuine task force to the real assembly site under cover of darkness and placed them under special camouflage covers. They were immediately replaced by prefabricated dummies to make it appear as though nothing had moved. On October 22 the remainder of the vehicles moved from the rear area to staging areas 40 kilometers to the south. That night the majority of vehicles moved to their real assembly areas in the north, leaving behind a mixture of real and dummy equipment to convince the Germans they were still in the south.
3) Supporting the "concentration" in the south with false radio traffic.

Montgomery's deception was a total success. Captured documents and German POWs placed three British divisions in the area where the fake concentrations were deliberately displayed. In fact, so convinced was the German Second Armor Division that the main attack would come in the south that they remained in the southern sector for the first four days of the attack.

### 1943 (Deception Operation: Lessons Learned)

In April, 1943, the Allies decided to carry out a deception scheme lasting the entire summer to keep alive in German minds the possibility of a cross-channel operation from Britain. This was meant to keep the pressure on Germany and cause the Germans to withdraw some forces from the Russian Front. In addition, the operation was to culminate in a feint attack to draw the Luftwaffe into an aerial battle at odds favorable to the Allies.

Throughout the operation, however, Germany took only the minimum precautions to repel a possible raid, and continued to move troops south into Italy and east into Russia. When the feint attack was launched on September 9, the Germans did not send up the Luftwaffe, and did not appear to believe the threat.

In reviewing what had gone wrong with the deception, the following problems were brought out:
1) The overall scheme had been devised by persons too far removed from the action such as the British and US Chiefs of Staff who had only slight knowledge of all it would entail.
2) The deception had tried to be too detailed and too realistic for the scale being simulated (a 10-division attack). The Allies were never able to simulate that size force by the time the feint took place. They continued to hope, or perhaps persuaded themselves, that the reduced scale would be effective.
3) There was an unnaturally fast build-up of the scheme: radio nets suddenly appeared, airfields sprung up daily, and clusters of boats appeared "out of nowhere."

The Germans saw through this poorly staged deception, but the

operation had given the Allies an idea of what was entailed in strategic-level deception operations. This new-found knowledge was to pay off the following year.

### 1943 (German Failure)

Sometime during 1942 and 1943, the Germans broke the telephone scrambler used by Churchill and Roosevelt over the transatlantic telephone. It was while listening to one such conversation that the Germans became aware that Italy had secretly approached the Allies about a separate armistice. During the first week of September, but before the 9 September surrender of Italy, the Germans made the mistake of murdering senior Italian military officers and taking charge of Allied prisoners in Italian hands. As a result of these actions, the US realized their scrambler had been unravelled. Another one was installed which the Germans were unable to break.

One can only speculate about what might have happened if the Germans had not compromised this source of intelligence, and had been able to learn the location of the D-Day landings.

### 1944 (The Invasion of Europe)

Following the deception fiasco of 1943, the Allies immediately began preparing the deception scheme for the actual invasion of Europe. The overall aim was first to give the impression that Allied attacks against the occupied countries could occur almost anywhere; then, when it became obvious that preparations were being made for a cross-channel invasion, to persuade the enemy that the main attack would be against Northeastern France or Belgium.

The Allies had learned their lesson about not rushing into a deception operation, and began their planning 11 months before the attack. They began occasional periods of radio silence to lower enemy vigilance when the actual attack came. They prepared dummy camps and deceptive lighting to simulate a gradual buildup on the British east coast, with a balancing concealment in the southwest where genuine assault forces would be concentrated.

As it became obvious that the attack would come from Britain, the Allies attempted to convince the Germans that the invasion would take place much later than planned. This was accomplished by the following means: 1) Stage managing questions in both the House of Commons and US/Canadian newspapers about a supposed shortage of landing craft; 2) Using "diplomatic indiscretions" about strategic bombing being so successful that there might not be a need to commit ground forces until late summer.

In 1944 it became known by reading the German code that the Germans considered Normandy one of the likely landing sites. The British then began a "double bluff," driving their deception efforts to show that Normandy might be one of several diversionary attacks preceding the main attack. This "main attack" would be aimed at the Pas de Calais (the most direct and, therefore, most likely landing site), some 200 miles east of Normandy. Through the use of false radio traffic and double agents who reported troops wearing different unit patches, a notional First USA Group (FUSAG) was created near Dover. These notional eleven

US/Canadian divisions were supposedly headed by General Patton. So sure were the Germans that Patton would be made Supreme Allied Commander that they saw FUSAG as the main attack force.

On the morning of June 6, 1944, as the invasion forces were enroute to Normandy, a diversionary fleet was also launched towards Calais. This "fleet" consisted of several small craft carrying radar jamming equipment and towing reflective balloons. These craft showed up on enemy radar screens as an invasion force 12 miles long and 8 miles wide. This scheme succeeded in two ways: first, it drew the majority of German coastal battery fire away from the actual forces; second, it convinced the Germans that it was an elaborate bluff to lower their vigilance when the actual Pas de Calais landing came.

To allow the Allies a chance to get a firm foothold in Normandy, the deception operations continued into mid-July, six weeks after the landings. Using propaganda broadcasts and reports by double agents, the British made the Germans believe that the main attack still had not occurred.

The detailed planning, gradual development, and continued support of the deception scheme allowed 47 divisions to eventually land in Europe, consolidate forces, and break out from the beaches with minimal resistance.

### 1950 (Chinese Intervention in the Korean War)

In mid-1950, United Nations forces under General MacArthur pushed virtually unopposed towards the Yalu River in an effort to destroy the enemy and unify Korea. Despite continued reports of contact with Chinese troops as he approached their border, MacArthur remained uncertain as to their strength, disposition, or intentions.

Chinese movement into Korea had been done under perfect OPSEC.

Moving only at night and avoiding all main roads, they had crept across country undetected by UN reconnaissance aircraft. During daytime halts they had maintained strict camouflage, noise, and light discipline. They had for the most part avoided contact. If taken prisoner, they maintained that they were "volunteers" who had come south to fight for Korea.

On November 25, when their attack began, the UN forces realized that there were six Chinese Armies (about 200,000 men) inside Korea. The Chinese had achieved near-total strategic surprise.

### 1967 (The Six Day War)

In June 1967, Israel launched a preemptive strike against Egypt. Within six days, the Israelis effectively destroyed the Egyptian Army in the Sinai, destroyed 90 percent of the Egyptian Air Force, and opened the Straits of Tiran.

**The number of persons with a "need to know" any particular information must be kept to a minimum.**

This was accomplished with the closely coordinated use of diplomatic and military deception. Moshe Dayan publicly stated Egyptian strength in the Sinai precluded a military reaction by Israel, and only diplomatic action was left. At the same time, the Israelis were mobilizing 264,000 men in 72 hours using coded messages over Radio Israel, and non-telephonic (word-of-mouth) call-up. The complete mobilization was done in secret.

In the days before the attack, the Israelis simulated a major buildup in the south. This they accomplished by moving tanks to the Gulf of Aqaba during the day, moving them 15 miles back into the desert at night, and then returning under Egyptian observation.

On D-1 Israel used electronic deception to cover the stand-down of all jet aircraft for maintenance and repair. By flying prop-driven planes emitting normal jet communication signatures, the Israelis hid one indicator of their intentions.

The massive Israeli success can also be blamed on poor Egyptian OPSEC. Through the use of electronic intelligence (ELINT) and air reconnaissance, Israel determined the best time to attack was 0845 Cairo time. The reasons for this were as follows:

1) The Egyptians always went on alert at dawn, expecting any attack to come at this time.

2) Combat air patrols were launched at dawn and other aircraft were placed on airstrip alert. However, by 0800 all aircraft had returned for refueling and maintenance.

3) At 0830 the alert was over and everyone was enroute to their normal duties.

4) Also, at 0830, Egyptian early warning radars were shut down for routine maintenance checks.

**The massive Israeli success can also be blamed on poor Egyptian OPSEC. Through the use of electronic intelligence (ELINT) and air reconnaissance, Israel determined the best time to attack was 0845 Cairo time.**

5) The Egyptian workday starts at 0900. At 0845 the Egyptian generals and unit commanders would still be enroute to their offices.

By establishing such predictable patterns, the Egyptian military had opened itself up to an Israeli strike.

## OPSEC LESSONS FOR THE FUTURE

By examining the past and observing which elements of protection, planning, and execution were instrumental in winning battles, we can get an idea of how best to direct our OPSEC efforts.

The way we train for combat is the way we will fight when the time comes. The next war will most likely be extremely short and intense. Therefore, we must begin beforehand to maintain security. Document security and physical security (to include restricted areas, barriers, and access control systems) must be seriously observed well before hostilities have broken out. The number of persons with a "need to know" any particular information must be kept to a minimum. When possible, avoid establishing patterns of operation. This is usually difficult to implement, because the military thrives on the SOPs as a way of making day-to-day operation less difficult.

Deception operations cannot be successful unless planned with the same degree of thoroughness as genuine operations. They must present a realistic and believable alternate course of action. The operation must begin early enough to allow a slow and natural buildup of action. The operation must begin early enough to allow a slow and natural build-up of a scheme. The scheme must be such that it can be supported with the men, material, and time alloted. The desired picture to be presented must be backed up with more than one source (radio traffic, agent reports, aerial photos) to verify the deception story.

Any radio traffic employed as manipulative communications deception cannot insult the enemy's common sense. The more challenging it is to the enemy intelligence experts, and the harder it is for them to break a code or establish a pattern, the more convincing it will become. The enemy intelligence expert is then more likely to believe, accept, and defend this "intelligence."

In preparing a diversionary attack, it is not always possible to commit a convincing enough force to deceive the enemy. Often, due to the force size available, it quickly becomes apparent that the movement is simply a diversion. It may be more profitable to convince the enemy that the real attack was simply a diversion, and the "main" attack will come later. This was done both at El Alamein and as part of Operation Overlord.

Surprise is one of NATO's most valuable assets in modern warfare; the ability to deny it to an enemy and to achieve it is the element of victory.

**Any radio traffic employed as manipulative communications deception cannot insult the enemy's common sense. The more challenging it is to the enemy intelligence experts, and the harder it is for them to break a code or establish a pattern, the more convincing it will become.**

FOOTNOTE

1. Anthony C. Bruce, **Bodyguard of Lies,** Harper and Row, New York, 1975, pp. 117-118.

BIBLIOGRAPHY

Cruickshank, Charles. **Deception in World War II.** Oxford, New York, Toronto: Oxford University Press, 1978.

Dulles, Allen. **The Craft of Intelligence.** New York, Evanston, London: Harper & Row, 1963.

Haldane, R. A. **The Hidden War.** New York, London: St. Martin's Press, 1978.

Hermes, Walter G. **US Army in the Korean War; Truce Tent and Fighting Front.** Washington: Office of the Chief of Military History, 1966.

Ind, Allison. **A Short History of Espionage.** New York: David McKay Company, Inc., 1963.

Kahn, David. **The Codebreakers.** New York: The Macmillan Company, 1968.

***Military Intelligence Magazine.*** Fort Huachuca, Arizona: US Army Intelligence Center and School, July-September 1978 (Vol 4, No. 3).

***Military Intelligence Magazine.*** Fort Huachuca, Arizona: US Army Intelligence Center and School, July-September 1979 (Vol 5, No. 3).

SupR 05069/80313, **Deception.** Fort Huachuca, Arizona: US Army Intelligence Center and School, 1979.

Winterbotham, F. W. **The Ultra Secret.** New York, London: Harper & Row, 1963.

# MULTIDISCIPLINE HOSTILE INTELLIGENCE SERVICE THREAT

by Major Richard L. Felling

**Counterintelligence threat analysis is highly complex. It goes way beyond the traditional equation of counterintelligence equalling counterespionage (CI=CE). Hostile intelligence services no longer rely on a single collection technique (discipline) to acquire information. The methods used range from the traditional human sources to a wide range of technical collectors employed on air, sea, land, and space platforms, and special operations and terrorism. The Army's Counterintelligence Production Division of the Intelligence and Threat Analysis Center (ITAC) views the threat from the hostile intelligence services as an integrated, well-coordinated, all-encompassing onslaught of intelligence and special operations activities.**

Boyce, Lee, Moore, and Kampiles: What do these Americans have in common? They were involved in transferring highly classified information to the Soviet Union. Fortunately, they were arrested before they could do more damage. But how many more people are actively involved in treason and collusion with hostile intelligence services?

The methods of intelligence collection, through human sources, such as the individuals already mentioned, or through spy satellites, the interception of radio signals, information gathering by embassies and consulates, auxilliary general intelligence ships, military aircraft, or even merchant shipping and commercial airlines, represent parts of a vast multidiscipline hostile intelligence network that is directed against the United States. The role of all hostile intelligence services—Soviet, East Bloc countries, Cuban, or Vietnamese—has traditionally been one of gathering information concerning the capabilities, vulnerabilities, and intentions of the United States Army.

Gone are the days when it was considered something of a game, exclusively for dashing cloak-and-dagger operatives always on the prowl for secret documents. Although the classical spying game does occur, it is only a small part of the current world of intelligence activity. Potentially hostile governments, principally the Soviet Union, are using every collection means at their disposal while reaching for intelligence superiority. The hostile intelligence threat faced by us today is multidisciplined, highly sophisticated, and extremely dedicated.

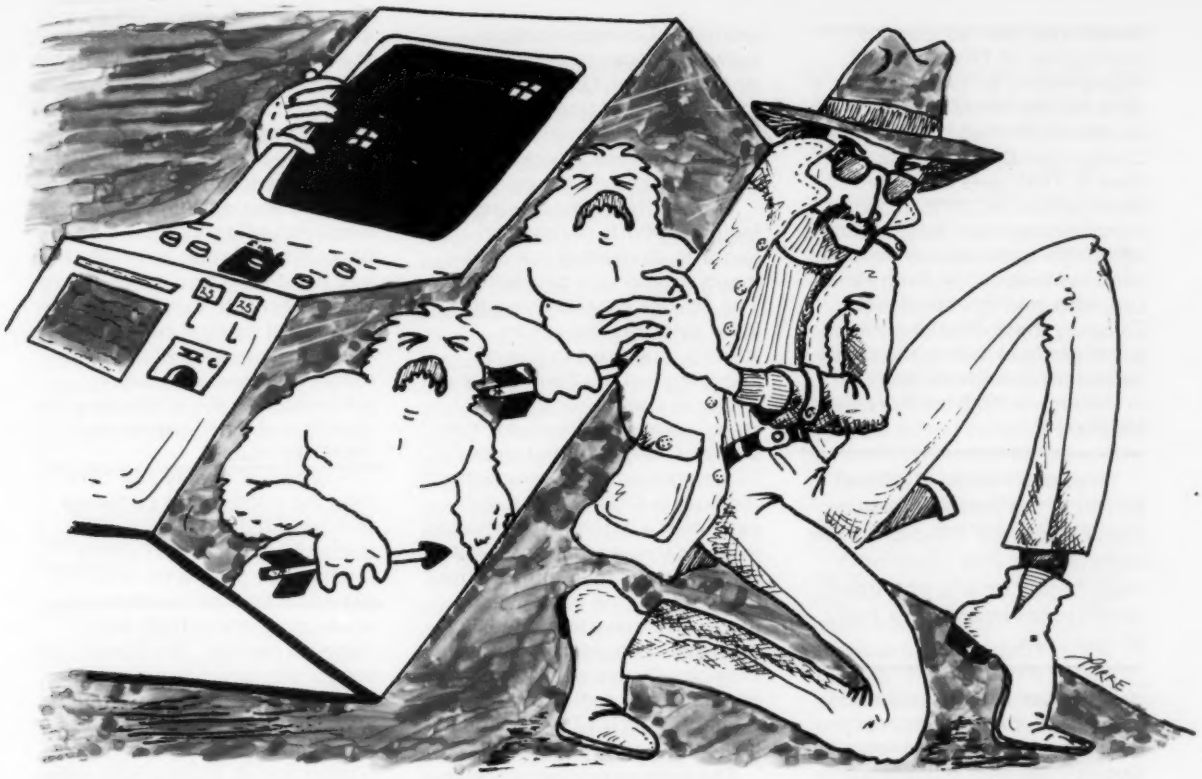
In their efforts to attain intelligence superiority, the hostile intelligence services employ the intelligence-gathering disciplines of Human Intelligence (HUMINT), Signals Intelligence (SIGINT), and Imagery Intelligence (IMINT). This three-pronged "collection attack" coupled with one additional activity, special operations (SPECOPS), is an ongoing program of worldwide subversion and special actions, contributing to a threat of ever-growing importance.

Although not all United States intelligence agencies agree on which discipline is the greatest threat to our security, overt HUMINT should be first. Overt HUMINT is the acquisition of information from open sources like news media, scientific magazines, trade publications, and contract specifications. These open sources provide about 95 percent of the hostile intelligence services HUMINT needs.

A US Senate staffer said of Soviet intelligence gathering on Capitol Hill, "They come all the time, but the number increases with the urgency of the information they want. You can see them asking the same groups of questions, as though they had memorized them."[1] The Soviets also attend open congressional committee hearings on defense, foreign policy, the economy, and just about every relevant aspect of American policymaking.

**Gone are the days when it was considered something of a game, exclusively for dashing cloak-and-dagger operatives always on the prowl for secret documents. Although the classical spying game does occur, it is only a small part of the current world of intelligence activity.**

The flow of technological information to hostile countries has increased significantly in recent years mainly because of the influence of detente. The sizeable legal presence in the United States of persons from hostile countries, and their freedom of movement, permits easier collection of information. The information obtained, along with the purchase of exportable, high



technology items, can be used to increase a hostile country's own military technology. Some examples of high-technology items that could be diverted to military use are miniaturized electronics, precision guidance systems, integrated electronic circuits, and wide-body jet engineering.

Clandestine HUMINT collection operations, intended to assure secrecy and provide plausible denial, are usually expensive and time consuming. They also involve potential political embarrassment for the sponsoring government if the operations are discovered. However, when the value of the desired information justifies the cost and risk, then the intelligence services do not hesitate to use this method.

For example, the Soviet KGB (Committee for State Security) searches for Americans in key spots who have exploitable weaknesses. KGB agents know they can probably blackmail or subvert an engineer who is trying to hide his homosexuality, a military officer with a yen for wine and women, or a diplomat who needs money. The hostile intelligence agent looks for two types of people: the person with influence and the person with access to classified documents. Government and military employees are prime targets, but scientists, engineers, and others, even hotel maids, are also objects of recruiting efforts.

The Soviets don't stop here. Within the past 5 years, many Communist attempts to subvert or recruit congressional staff members have been detected. Recently, one such case was discovered when a noted congressman was interviewing personnel for positions on the Permanent Select Committee on Intelligence. One individual with outstanding qualifications and recommendations was selected. The congressman routinely checked with the FBI. The highly qualified future staffer was in fact a paid, controlled agent of the East German Intelligence Service.[2] Within the subcommittee, he could have betrayed secrets, and more significantly, he could have affected national decisions about important issues.

The human characteristics exploited by hostile intelligence services are as follows: greed, psychological instability, and resentment against the United States government. One person who displayed such characteristics was Edwin G. Moore II, who attempted to pass a name list of 300 Central Intelligence Agency employees and other agency documents. Moore, a former CIA employee, asked for $200,000, in return for which he would provide more classified documents. Fortunately, Moore was arrested and the documents were recovered.

Another person was the CIA watch officer, Michael Kampiles, who had access to important documents. Kampiles sold a top secret technical manual describing the capabilities of one of our intelligence satellites to the Soviets for a mere $3,000.

A good example of the Soviet's ability to exploit character weak-

nesses was their successful penetration of TRW Systems Incorporated, a major supplier of advance electronic military equipment to the US Air Force. Christopher Boyce, a security clerk at TRW, was convicted of stealing Top Secret microfilms from his employer. Boyce transferred the material to an accomplice in Mexico City, Andrew Lee, who sold it to the Soviet Embassy there. The two men acknowledged selling the classified information from April 1975 to December 1976 for more than $80,000.[3]

**To exploit these COMINT sources, the Russians have converted their US diplomatic installations into electronic espionage centers equipped to intercept microwave telephone calls.**

The second of the collection disciplines, SIGINT, incorporates several subcategories: Communications Intelligence (COMINT), Electronic Intelligence (ELINT), and Telemetry Intelligence (TELINT). TELINT is now officially re-christened "FISINT" (Foreign Instrumentation Signals Intelligence). COMINT has the greatest impact on our day-to-day job performance. Prime sources of valuable COMINT include both nonencrypted and encrypted telephone and radio messages.

To exploit these COMINT sources, the Russians have converted their US diplomatic installations into electronic espionage centers equipped to intercept microwave telephone calls. Tapes on which thousands of transmissions have been recorded are flown back to the Soviet Union in diplomatic pouches. There they are fed into huge computers keyed to sort-out calls to or from American telephone numbers of interest to the KGB.

ELINT is information derived from noncommunications electromagnetic radiations, such as those emitted by radar. TELINT is derived from the intercept and analysis of communication between pieces of equipment. An example of TELINT would be information obtained from the intercept of electronic communications between a rocket and its ground-based guidance system.

The SIGINT mission also includes efforts to monitor, degrade, or destroy our command and control capabilities. The Soviets may have hunter-killer satellites, known as ASATS, that are capable of knocking out the Pentagon's ability to communicate with ships, planes, submarines, missile silos, and ground forces. The magnitude and versatility of the hostile SIGINT effort indicates that a highly sophisticated threat is targeted against United States' armed forces throughout the world. In the past 5 years, the Soviets have launched 325 satellites for possible military missions. These satellites may be capable of performing numerous SIGINT collection tasks throughout the world.

The third collection discipline, IMINT, can be collected not only from space but also from land, sea, and air platforms. The most serious threat from hostile IMINT resources at the strategic level comes from photoreconnaissance satellites. Under present international law, space is open to all. It also has, by its nature, positional dominion over the entire surface of the earth. International borders and the rule and restrictions that a nation may impose to keep its secrets do not apply to the realm of space. Consequently, it is an extremely favorable environment for intelligence collection operations—if a hostile intelligence service has the resources and technology to use space.

Soviet IMINT collection is performed virtually on a daily basis. Hand-held photography is used to confirm military targets at close range. Thousands of Communist tourists, official visitors, and diplomatic personnel use this method to obtain photography of our military and industrial installations. The deployment of reconnaissance aircraft off our coasts provides the hostile country with valuable information. At the tactical or field combat level, airborne collection poses the greatest threat. The Soviets use numerous aircraft types to obtain radar imagery and photography of deployed military units. This capability together with satellite and hand-held photography provides them with location, disposition, and combat capability. Technical equipment improvements are constantly being achieved, thereby enhancing the quality and timeliness of the IMINT product.

A potential enemy can combine the information collected through SIGINT with the products of HUMINT and IMINT intelligence programs, and can provide a flow of coordinated, all-source data to high-level decision makers. The threat from sensor-equipped and photographic satellites, spy ships, microwave generators and receivers, tiny listening devices, and human agents plays a fully integrated role in today's espionage operations.

In their rational and scientific approach to military problems, the hostile intelligence services planning staffs have not forgotten the importance of SPECOPS. The SPECOPS missions may involve sabotage, unconventional warfare, subversion, assassination, disinformation, and other operations not related to collection. The abundant, unclassified Soviet military literature that deals with the conduct of modern combat barely mentions airborne employment of clandestine sabotage methods. The Soviets are well aware of the value and importance of guerrilla and clandestine operations behind enemy lines. They have stated officially that the Soviet partisans in WW II were responsible, through their clandestine activities directed from Moscow, for the destruction of 20,000 railroad trains and 12,000 railroad and highway bridges, for the disabling of 4,000 tanks, and for the killing or wounding of 1,000,000 "fascists." However, in

current Soviet military articles, the role of planned clandestine operations has been maintained in absolute secrecy.

The first of the SPECOPS categories, sabotage, must be divided into two broad and distinct elements: that which involves intelligence participation and that which embraces sabotage from all other sources. The threat of sabotage controlled or activated by hostile intelligence is greatest during crisis, pre-war, or wartime conditions, and requires extensive, sophisticated countermeasures.

**Subversion can occur during either peacetime or wartime.**

A unique potential threat comes from Warsaw Pact (WP) forces which have been especially trained for long-range reconnaissance and sabotage missions. Their targets are ports and harbors, rail lines, highways, and airports. Sabotage units are a special part of the regular WP forces, and are capable of preparing, supporting, and complementing overt aggression through covert action. Because of the secrecy surrounding them, confirmed intelligence on the makeup and mission of these forces is limited.

Nonintelligence-sponsored sabotage is usually criminal in nature, and poses a threat of varying proportions at all times. It is best guarded against by standard security measures.

In addition to sabotage, unconventional warfare operations may be activated before, or at the outset of, hostilities. Hostile intelligence agents-in-place can be prepared to initiate guerrilla warfare, assassination, and subversive activity using local dissident elements, political sympathizers, and other activists. Hostile intelligence subversive activity is designed to achieve influence, which can be expanded so that the subversive movement can seize, destroy, control, or achieve a lesser intermediate objective. It will normally begin with agitation, expand to propaganda, and then culminate in action.

Subversion can occur during either peacetime or wartime. A hostile intelligence service would rely heavily on communist parties, dissident elements, front organizations, and "friendship societies" for such operations. They would sow confusion among the population at or before the onset of hostilities, thereby making it difficult for the target government authorities to act effectively.

During crises, pre-war or war, assassination and kidnapping controlled by hostile intelligence services would play a major part in the accomplishment of an overall mission. Operations conducted in a clandestine manner (made to appear as accidents or criminal acts) would eliminate key government personnel in leadership positions. Again, such operations are conducted to demoralize and terrorize the civilian population and the authorities.

Although not as significant, peacetime assassination and kidnapping operations do take place. Vladimir Kostov, a defector to the West and a former member of the Bulgarian Communist Party, was shot by the Bulgarian Secret Intelligence Services at a Paris Metro station. The weapon used was a fountain-pen-shaped object that fired a poison-filled metallic ball about the size of a pinhead into Kostov's back. Another Bulgarian defector, writer, and commentator, Georgi Markov, was shot in London by an attacker using an umbrella apparently designed to fire a metallic object about the size of a pinhead.

The last category of SPECOPS, disinformation, involves the dissemination of false, incomplete, misleading, and provocative information by clandestine means. During questioning, Arkady Shevchenko, the highest ranking Soviet official ever to defect to the West, stated

**Although not as significant, peacetime assassination and kidnapping operations do take place.**

that the KGB has a specialized department that deals only with disinformation. Forgery would play an important role in the spread of falsehoods.

We must recognize how far our potential enemies will go to gather information about us. Threats posed by hostile intelligence services cannot be underestimated. These services are highly aggressive and dedicated. They use a many-layered structure and a multidiscipline collection effort to accomplish their missions. Evidence suggests that hostile intelligence services are engaged in their greatest offensive ever in the United States. A nation like ours, with its open society, is more vulnerable to the theft of its vital information; consequently, we must constantly be aware and on guard. The multidiscipline hostile intelligence threat is real; if we fail to recognize it, we do so at our own risk.

1. *Soviet KGB in America*, by Howard Handleman, ***Air Force Magazine***, June 1979, page 59.
2. *Espionage: Dark Side of Detente*, by John Barron, ***Reader's Digest***, January 1978.
3. Robert Lindsey, ***New York Times***, 29 April 1979

**MI Prospectus**

Additional copies of the January-March 1981 issue of Military Intelligence Magazine are available to units/activities who are interested in recruiting or for informing current MI personnel on career development opportunities.

If copies are needed, please write:

**Commander**
**USAICS**
**ATTN: ATSI-DOS-LGT (Mr. Willsey)**
**Fort Huachuca, AZ 85613**

To speed delivery of your request, please include a mailing label addressed to your unit.

-Editor-

# ACSI viewpoint

by Major General Edmund R. Thompson

In response to an outrageous breach of trust by a public official, a Chief Justice of the Supreme Court once observed, "Secrecy in government is the incubator for corruption." In a trade where secrecy, stealth, and anonymity are often the prerequisite of success, today's intelligence community must face the test not merely of professional competence, but of maintaining public confidence in the need for confidentiality.

The Freedom of Information Act (FOIA) and the Privacy Act have put the onus of persuasion directly upon the Intelligence Community to prove the need for secrecy. Rubber stamps and red ink alone will no longer suffice, and ignorance or misuse of the classification system designed to protect national defense information is the surest path to court-ordered disclosure and the loss of public confidence in our need for secrecy.

The FOIA and Privacy Act are not inherently bad laws. Quite the contrary, both are a demonstrative step to reinforce a fundamental concept of democracy: That the government and the information of government belong to the people. During the infancy of our Republic, James Madison wrote, "A popular government without popular information, or the means of acquiring it, is but a Prologue to a farce or a tragedy; or perhaps both. Knowledge will forever govern ignorance; and the people who mean to be their own Governors must arm themselves with the power which knowledge gives." Nearly two centuries hence, nothing has changed to alter Mr. Madison's axioms; what has changed are the needs of society to defend its very survival by accomplishing a portion of that defense outside the immediate limelight of public scrutiny. The FOIA and the Privacy Act acknowledge this and provide for exceptions. The Intelligence Community more so than other arms of the Executive Branch of government must be aware of these exceptions and understand their intent.

Perhaps one of the more startling aspects about the two acts is the recency of their enactment. The postulations of Mr. Madison and others aside, until passage of the FOIA the burden was on the individual citizen to prove his right to look at government records. Our familiar "need to know" was the criterion for release, with the burden of proof to establish that need placed on the individual citizen. Government agencies were authorized to keep information secret, "for good cause shown" or where secrecy "was in the public interest."

Perhaps more importantly, there were no statutory guidelines to assist individuals seeking information, and no judicial remedies available to those wrongfully denied access. In 1966, Congress sought to remedy this situation with passage of FOIA, making it clear it was the intent of Congress that *any person* should have access to certain records without having to demonstrate a need or even a reason. What some perceived as "government foot-dragging" and the tragedy of Watergate produced a series of amendments to the original legislation in 1974, over the veto of President Ford. These encouraged even more disclosure than the original statute.

The FOIA is composed of five subsections. If a request for information is adequately drawn and properly presented to an agency of the Executive Branch—which includes the Military Departments—disclosure is mandatory unless the information is deemed to come within the purview of nine exemptions found in subsection (b) of the

Act. Two of these have significant impact on the confidentiality of intelligence operations and plans:

Exemption One covers classified documents concerning national defense information and foreign policy. The test for application of this exemption is: the document is (a) specifically authorized under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy, and (b) is in fact properly classified pursuant to such executive order. The document must fulfill *both* portions of the test to be declared exempt from disclosure. Prior to the 1974 amendments of the FOIA, the mere fact that a document was classified (i.e., bore classification markings) was often sufficient for it to fall within the exemption. Now, an individual may appeal a withholding make on those grounds. In such cases a judge will make an independent determination of the applicability of Exemption One, and the burden is on the government to convince the court the document is properly classified.

Exemption Seven covers "investigatory records" compiled for "law enforcement." (For the purpose of the Act, personnel security investigations are deemed to be for law enforcement purposes.) Disclosure is required unless one of six "harms" can be demonstrated. Of interest to the Intelligence Community are exemptions which (a) protect the identity of confidential sources, and confidential information furnished only by the confidential source, in the course of a lawful national security investigation, and (b) protect against the disclosure of investigative techniques and procedures. The nuances of the protections afforded to confidential sources should not be overlooked. In some circumstances the identity of a confidential source can be protected, *but not the confidential information furnished.* Happily, the courts have not demanded an express promise of confidentiality to protect the identity of a source; his identity can also be protected if he provided information in circumstances from which an assurance of confidentiality can reasonably be inferred.

In 1975, Congress bolstered the concept of freedom of information with passage of the Privacy Act. The distinction between FOIA and the Privacy Act is that while the former was intended to make available *all* types of information, the Privacy Act was intended to assist individuals in obtaining information about *themselves.* The legislation is designed to give citizens a greater voice in what information about them is collected by the Federal Government, and to what purpose that information is put. As with FOIA, the act applies only to the Executive Branch of government. The mechanics of disclosure are very similar to FOIA.

Undoubtedly, the Acts have been subject to abuse. Unfortunately, more is known of successful abuses by the criminal element than by hostile intelligence services. FBI Director William Webster has reported at least 6 percent of all FOIA inquiries filed with the FBI come from prisoners who are trying to figure out who supplied the confidential information which resulted in their detention. In at least one documented case, a witness in a muder trial, relocated and provided with a new identity by the FBI, was unmasked by an FOIA inquiry.

In a deliberate attempt to illustrate the weaknesses of present legislation, an OPSEC support mission for a special research and development program submitted 40 FOIA requests over a two-year period. Responses led investigators to two entire systems found to be in open-source literature. Keying on these systems, additional FOIA requests revealed performance characteristics for a new light tank, contract information concerning test vehicles, and the physical characteristics of a high mobility and agility test vehicle and light tank.

Fortunately, not all attempts to manipulate FOIA have been so successful. In cases recently decided by a Federal Court of Appeals in Washington, DC, attempts by a self-appointed watch-dog organization and Rolling Stone Magazine failed to force disclosure details of the Glomar Explorer expedition by the CIA.

Currently undergoing congressional hearings are two legislative proposals to amend the FOIA. The first would amend the National Security Act of 1947, and create an exemption from disclosure, records of agencies involved in foreign intelligence or counterintelligence activities. A second proposal would, among other things, restrict application of the FOIA to US persons, and provide an additional exemption for sensitive unclassified materials.

Regardless of the outcome of these proposed changes, it appears that certain mandatory disclosure laws have the unequivocal support of Congress. For the Intelligence Community to maintain the secrecy which is the *sine qua non* of our trade, we must scrupulously adhere to the requirements of the allowable exemptions to disclosure, thereby maintaining public confidence in their continued worth.

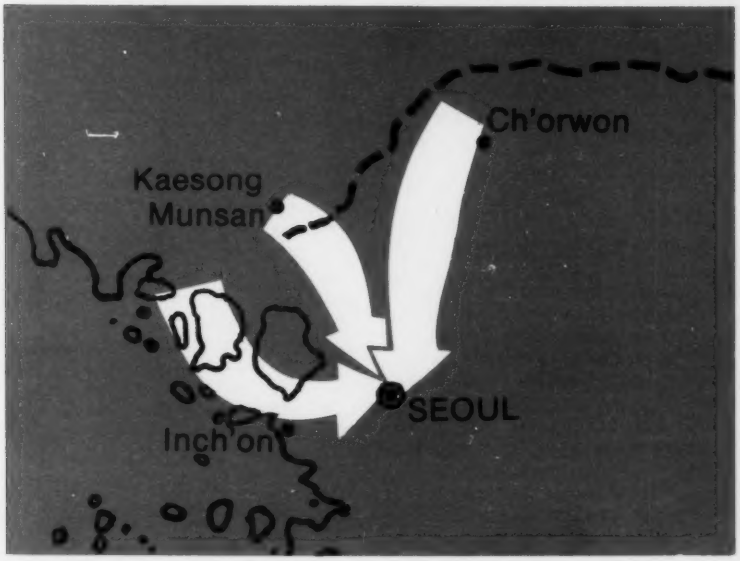
# North and South Korean OB

by Thomas A. Marks

This article presents an analysis of the order of battle figures for the Democratic Republic of Korea (North Korea) and the Republic of Korea (South Korea). Quantitative pairings tell part of the story. Forces must also be considered from the qualitative perspective which has two components: consideration of weapons systems themselves and consideration of them in their probable role on the battlefield. The following qualifications apply to this study: first, this study is not intended to go beyond the tactical level, and it ignores political, strategic, micro-geographic, and economic considerations; second, optimum performance of weapons systems must be assumed in the absence of specific information to the contrary; third, this study examines both sides on their individual merits and does not allow for outside intervention.

The answer to the following question is important: At this point in time, do the South Koreans have the capability to defend themselves against a North Korean attack? An assumption is made that North Korea will attack South Korea. This is a valid assumption and is justified by the force dispositions and the activities of both sides over the past decade.

Hundreds of incidents started by North Korea have marred the armistice, which ended the Korean War in July 1953. Further, North Korean forces are not placed to repel an attack against their homeland. Instead they are already forward deployed and give every indication of being positioned to provide maximum flexibility for offensive operations.[1] In contrast, the South Korean forces are deployed so that they are only capable of defensive operations and limited counterattacks.




**Attack.** The primary objective of any North Korean assault on South Korea would be Seoul, the political-economic heart of the country (see above). There are three primary invasion routes:

1) The Chorwon Valley—the traditional invasion route to the South used by the North in its 1950 assault.
2) The Kaesong-Munsan approach—a shorter route from the North Korean textile town of Kaesong through the Munsan road junction (about 35 km from Seoul).
3) Through the Han Estuary.

US sources consider the Kaesong-Munsan approach to be the most likely invasion route.[2] Although it is only one-third as wide as the Chorwon Valley, it is the shortest and most direct route. In contrast, the Chorwon Valley route is 85 km long and difficult to travel on. Also, supply connections to this route are limited. The Kaesong-Munsan route has several good supply routes. The Han Estuary is subject to the second highest tidal fluctuations in the world. Therefore, because of limited North Korean amphibious capabilities, it would be a poor choice as an attack path.

Regardless of the approach, considerations of terrain would be similar for both land routes (options 1 and 2). A main attack would be supported by strong secondary thrusts along the alternative routes, for deception and to prevent South Korean forces from shifting to mount a counterattack. Simultaneously, specifically trained light infantry brigades would infiltrate South Korean rear areas. The navy would support amphibious raids and probes, and perform interdiction missions. The air force would attempt to strike targets of both a tactical and strategic nature. North Korea's superior air defense system would provide protection for the North's rear areas.

**Relative Strengths.** The most recent public estimates of North Korean forces available for an attack are shown in Table 1. South Korean defense forces are listed in Table 2. Although the South has a superior mobilization potential because of its greater military-age population, its call-up procedures are such that additional forces would not be available in the critical early rounds of fighting. Furthermore, the chances of the North achieving surprise are very high, thereby ensuring that the contest would be fought between existing forces during the initial stages of battle. A surprise attack would allow the North to have its own paramilitary forces already mobilized.

**TABLE 1**

**KOREA: DEMOCRATIC PEOPLE'S REPUBLIC (NORTH)**

Total armed forces: 678,000.
Estimated GNP 1980: $10.5 bn.
Defence expenditure 1980: 2.74 bn won ($1.3 bn).*
$1=2.05 won.

Army: 600,000.
8 corps HQ.
2 tk divs.
3 mot inf divs.
35 inf divs.
3 AA arty divs.
4 armd bdes.
4 recce bdes.
4 inf bdes.
8 lt inf bdes.
22 special forces (cdo) bdes.
2 indep tk regts.
5 indep inf regts.
100 arty bns.
82 rocket bns.
4 SSM bns with FROG.
1 river crossing regt (3 bns).
3 amph bns (engrs).
5 AB bns.

RESERVES: 260,000; 23 divs.

Navy: 31,000.
16 submarines.
4 Najin frigates.
18 ex-Sov FAC(M).
25 large patrol craft.

RESERVES: 40,000.

Air Force: 47,000; 615 combat aircraft.
3 lt bbr sqns with 85 Il-28.
13 FGA sqns with 20 Su-7, 340 MiG-15/-17/-19.
12 interceptor sqns with 120 MiG-21, 50 MiG-19.
Tpts incl 200 An-2, 40 An-24, 10 Il-14/-18,1 Tu-154.
4 SAM bdes (40 bns) with 250 SA-2 in 45 sites.
Para-Military Forces: 38,000 security forces and border guards; civilian militia with small arms, some AA arty.

*It is uncertain whether this covers all defence expenditure, and there is no consensus on a suitable exchange rate for the dollar conversion.

**THE MILITARY BALANCE,** International Institute for Strategic Studies, 1980-81.

**TABLE 2**

**KOREA: REPUBLIC OF (SOUTH)**

Total armed forces: 600,600.
Estimated GNP 1978: $46.0 bn.
Defence expenditure 1980: 2,010 bn won ($3.46 bn).
$1=580.5 won (1980), 484 won (1978).

Army: 520,000.
5 corps HQ.
1 mech inf div.
20 inf divs.
2 armd bdes.
2 indep inf bdes.
7 special forces bdes.
2 AA arty bdes.
7 tk bns.
36 arty bns.
2 SSM bns with Honest John.
2 SAM bdes (3 HAWK, 2 Nike Hercules bns).
1 Army Aviation bde.

RESERVES: 1,100,000; 8 inf divs (cadre).

Navy: 48,000 (incl 23,000 Marines).
10 ex-US destroyers.
7 ex-US frigates.
6 ex-US corvettes.
8 FAC(M) with Standard SSM.
10 large patrol craft: 2 100-ft, 8 ex-US Cape.
Coastguard: 25 small craft, 9 Hughes 500D hel.

RESERVES: 25,000.

MARINES: 23,000.
1 div.
2 bdes.

RESERVES: 60,000.

Air Force: 32,600; 362 combat aircraft.
16 FB sqns: 4 with 60 F-4D/E, 10 with 220 F-5A/B/E/F, 2 with 50 F-86F.
1 recce sqn with 12 RF-5A.
1 ASW sqn with 20 S-2 F.
C- Tpts incl 12 C-46, 10 C-54, 10 123, 2 HS-748 Aero Commander.

RESERVES: 55,000.

Para-Military Forces: A local defence militia, 2,800,000 Homeland Defence Reserve Force.

**THE MILITARY BALANCE,** International Institute for Strategic Studies, 1980-81.

Over the years, South Korean force levels have remained essentially static; those for the North have grown. There is also a trend towards increasing disparity between North and South Korean military levels. This gap can only increase, given the North's extensive dedication of resources and effort to the creation of a military machine, which is now self-sufficient in some areas of production.

Limited domestic weapons and armament production capabilities exist in both countries, but neither of the antagonists would be capable of any massive infusion of additional combat factors. Estimates are that the North could sustain mid-intensity combat operations for 90 days without resupply; the South for 30 days. The South, in defending its positions, would have the advantage of shorter supply lines and a better transportation infrastructure. Both sides would find their repair capability hampered because of their dependence upon external sources for many parts.

**Armor.** The spearhead of any North Korean attack would include the North's superior armor forces. Most North Korean tanks are Soviet-manufactured T-54/55s or Chinese-manufactured copies of these models, such as the Type 59. Some T-62s, however, have been deployed following their in-country manufacture. These are tough fighting machines, with good construction range, but they do have flaws. A poor gearbox, manual traverse, lack of a turret basket, requirement for top-loading, thin armor, poor crew operating conditions, obsolescent main armament (in the case of the TD-54/55), and vulnerable ammunition and fuel storage are some of the flaws. These discrepancies have proved to be quite important in actions where Soviet tank designs have met their American counterparts, such as in the Yom Kippur War of 1973 in the Middle East.

Despite these facts, the T-54/55 cannot be classified as an inferior machine. Continued upgrading has been incorporated into the design during production runs, and the engines and guns of at least some tanks have been replaced with more modern equipment, a standard procedure which has also been followed with South Korean tanks.

The remaining part of the North Korean Armor force contains older tanks, T-34/85s, PT-76s, and Chinese Type 62s (a light tank unlike the Soviet T-62 forces). The T-34, though old, is still widely regarded as the best all-around tank for its age. Indications are that it would serve as the cutting edge of North Korean spearheads, using its still formidable assets to wear down South Korean armor resources before North Korean commitment of T-54/55 and T-62 forces.

Although designed as a light tank for reconnaissance work, the Type 62, with its 85mm main gun, the same as that possessed by the T-34, could also perform a role such as that planned for the T-34. The rugged terrain of the approach routes to Seoul would enhance its mobility and its chances of survival. The armor and small 76mm gun of the PT-76 amphibious tank make it unsuited for action against main battle tanks; its role would be reconnaissance.

South Korea's armor forces are comparable to those of North Korea in quality, but tables I and 2 show that the South is outnumbered in this category by a 2:1 ratio. Twenty percent of the South Korean tank force consists of M-47s. The M-47, despite its age, is still in wide service and has earned a reputation for mechanical reliability and good mobility. The 90mm gun is a reasonably effective weapon and in some cases has been replaced with the 105mm cannon. The basic ammunition load for the 90mm gun is 71 rounds (as opposed to the T-54/55's 43 rounds), and removal of the bow machinegun allows for storage of 105 rounds total, a tremendous operational advantage.

South Korean M-48s, the remainder of the armor force, are all of the M-48A5 version. This design includes the fitting of a 105mm gun, T142 track, modified ammunition racks, gun travel lock, and numerous other improvements. There are plans to increase ammunition storage from the previous 63 rounds, and the engine has in many cases been "hyped." The M-48, as demonstrated by its service in Vietnam and in the Middle East Wars, has proved to be a highly satisfactory weapon.

The M-47s and M-48s have a number of advantages over the Soviet designs used by North Korea. In the Yom Kippur War, the superior ammunition load of the US-made tanks, combined with their superior rate of fire, frequently tipped the scale in engagements. The improved storage capacities being fitted to both the M-47 and M-48 should increase this advantage.

American designs have also proved less susceptible to fire, even though their increased fuel capaci-

ties have increased their operating ranges (482 km for the M-48A5). Turrets of the M-47s and M-48s are less cramped than those of Soviet tanks, possess a turret basket and automatic traverse, and do not require top-loading (elevating the main gun after each shot to lower the breach for insertion of a new round). They possess superior aiming optics, particularly for night fire. Although the theoretical first-round hit probabilities of the American and Soviet models are comparable, in practice the former has proved capable of faster engagement.

Complementing South Korea's main battle tanks are a number of M-41 light tanks with 76mm guns. Their armor protection is superior to that of the PT-76, which would give them a higher survivability factor in a mid-intensity combat environment. They would still have to be used in reconnaissance, because they would be no match for North Korean main battle tanks. Conversion of the main gun to one of heavier caliber would enhance their value.[3]

Fleshing out North Korean tank forces would be roughly 100 to 200 assault guns of various calibers: the SU-76, SU-85, and SU-100 (the numerical portion of the designation indicates the caliber of the main armament). Designed to beef up the firepower of armored columns, these can engage South Korean armor. The South has no comparable machines, but does have some M-18 self-propelled antitank guns with 76mm armament. These antitank guns would have limited impact on North Korean armor unless refitted with a heavier gun.

**Infantry.** Accompanying the armor forces would be infantry in a variety of armored personnel carriers (APCs) and on foot. Although a South Korean infantry division is larger than its North Korean counterpart, roughly 15,000 men versus 10,000 men, the armament possessed by both is essentially equivalent. Thus the South would be heavily outnumbered and outgunned (North Korea now has twice as many infantry divisions as the South). In recent years, the North has concentrated on developing mechanized infantry forces and now has three motorized divisions[4] compared to the South's one. Armored personnel carriers in North Korea's inventory include indigenous designs similar to the US M-113 APC. These are the M-1967 and M-1973. The significance of these vehicles lies less in their characteristics than in the fact that they are locally designed and constructed. Other troop carriers include the Soviet BRT-40, -50, -60, and -152.

South Korean APCs are primarily M-113s. Neither Soviet nor US APCs will be considered in detail here, because both groups used by the two Koreas are essentially "armored taxis," used for carrying large bodies of infantry into the vicinity of the battlefield with some slight armor protection. There they are left to proceed on foot.

Later Soviet models not possessed by the North Koreans yet, such as the BMP, have been designed to accompany tanks into the assault and onto and beyond the objective. These are armored fighting vehicles (AFVs), and the US has followed the Soviet lead by developing its own version. It is most likely a matter of time before the North and South Koreans follow the development trend established by their major weapons suppliers.

This will probably also be true in the areas of electronic warfare (EW) and nuclear, biological, and chemical (NBC) capabilities. Both sides presently have EW assets and the capability for limited offensive and defensive chemical operations. North Korea considers signal intelligence a primary source of data, and is capable of searching all friendly frequency bands and locating units through numerous direction-finding sets. Both ground and air assets are used. The Soviet doctrine of radio-electronic combat (REC) is practiced. In contrast, South Korea follows the US lead and is more committed to the long-term exploitation of continuous-source monitoring.

In NBC operations, the North would have the advantage of the Soviet experience with chemical weapons in Afghanistan and the Vietnamese experience in Laos and Cambodia. In these areas, NBC employment techniques have been tested, and it would not be surprising to see a North Korean attack resort to such weapons, for which the South Koreans are largely unprepared.

A further component is the use by both sides of overt, or uniformed, unconventional warfare groups. The North has 8 light infantry brigades and 22 commando brigades, each comprised of approximately 300 highly trained officer specialists whose mission is reconnaissance behind enemy lines and the disruption of enemy rear areas. These forces are trained for infiltration by any mode, and have already made numerous raids into the South on special missions.

South Korea itself fields seven Special Forces brigades, which perform functions like the North Korean light infantry brigades. Also, the former are charged with the destruction of the latter, when such elements exist, despite efforts by regular units to eliminate them.

**Artillery.** The North has an artillery advantage which is so great that it is difficult to measure. As figures extracted from the tables indicate, relative artillery strengths overwhelmingly favor North Korea. Even more significant are the North's long-range weapons which can fire more than 15 km. The North has hundreds of these weapons, but the South has only 60. This would allow the North's weapons to maintain their prepared positions, constructed of concrete or dug into rock, while covering an advance. This would not only increase their survivability, but would increase their accuracy. The South's artillery, with its much shorter ranges, would not provide effective preplanned fires or counterbattery missions.

The North has a limited capability for manufacturing its own self-propelled artillery. Although it is not evident from a comparison of artillery pieces alone, there is an even more stunning imbalance in the tubes available to the North as compared to the South because of the former's possession of 1,900 multiple rocket launchers (MRL) of various sizes, a weapon not found in the South Korean inventory.

Augmenting the artillery on both sides are free rocket over ground (FROG) rocket forces. The North has several dozen FROG-3/5/7s with ranges between 36 and 60 km. The South has the American *Honest John* (range 38 km) and a locally produced model for which performance data is not available. Both the FROG-5 and FROG-7 can hit Seoul from present locations, and both

may be armed with a variety of warheads, though only conventional rounds are currently in the North's inventory. FROGs would probably be used to attack enemy force concentrations and rear area deployments of troops and armor. The South would use its rockets in a similar fashion. To increase the value of its rocket forces, it is replacing the *Honest John* with the more modern *Lance* and *Sergeant* guided missiles, which have superior range and accuracy.

**Antitank.** The preceding data for ground forces indicate that the South Koreans are at a considerable disadvantage. Faced with similar unfavorable odds in Europe, the NATO forces have reinforced their antitank weapons and airpower. This path has also been taken by the South. Both the North and the South possess antitank guided missiles (ATGMs) developed and manufactured by their respective supporters the USSR and the US. The South Koreans have the TOW (tube-launched, optically-tracked, wire-guided antitank missile), and the North Koreans have the Snapper. Both sides have attempted to gain additional advanced models.

Although the US has not yet provided the Dragon or Shillelagh missiles, the USSR may have given the Sagger to the North. Nevertheless, the South Koreans have an advantage in this area, because the TOW has superior range and accuracy, particularly against moving targets.[5] When registering a hit, however, either the Snapper or the Sagger can penetrate any known armor, and both have kill probabilities of nearly 70 per cent (the comparable TOW figure is reported to be in excess of 90 per cent).

To complement the space not covered by antitank missiles and guns themselves, a variety of weapons are used. Particularly valuable for the North Koreans are the 368 RPG-7s found in each basic infantry division. This weapon has been used worldwide. It is usually compared with the US LAW (light antitank weapon), because the functions of the two in battle are similar. The RPG-7 is an assigned weapon reloaded by the user, but the LAW is classified as a round of ammunition and cannot be used again after being fired. Both the RPG-7 and LAW have accuracy problems at long ranges, but the RPG-7 has a greater first round hit probability at greater ranges than the LAW.

Despite a slight South Korean edge qualitatively in the overall antitank weapon area, the overall balance on the battlefield does not appear to have been decisively changed by figuring in this factor.

**Airpower.** A second element which could be used to offset the North's superiority in armor and artillery is airpower. The actual uses of air superiority are numerous, from close air support of ground forces to air interdiction of supply lines. The North has an edge in total combat aircraft, 615 compared to 362, but nearly half of the North Korean planes are outmoded MIG-15s and MIG-17s, both introduced in the late 1940s.

Regardless of their armament, these aircraft are no match for the newer models in the South Korean inventory, the F-5E and F-4D/E. In fact, given the age of the planes, it is likely that many have already reached the limit of their airframe lifespans and would be incapable of even carrying bombs. They could certainly not be used effectively as interceptors unless willing to accept maximum casualties. It would nonetheless make sense, from the North Korean standpoint, to throw as many of these aircraft into the fight as possible to score at least some hits against the South Koreans. This is so because the MIG-17 has an all-weather capability not possessed by the newer MIG-19.

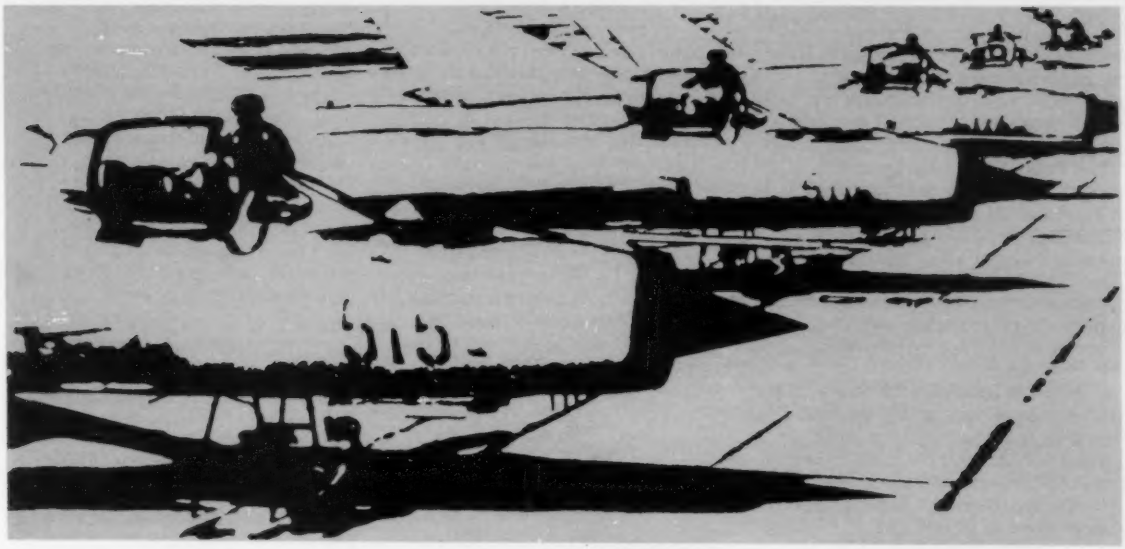
Remaining North Korean fighters are comparable to the South's models. The main threat is posed by the MIG-21s and MIG-19s, although the latter are growing old, having already gone out of production in the USSR. The MIG-21, which has an all-weather capability, was found by the Egyptians to be a troublesome aircraft in combat. Further, both the MIG-19 and MIG-21 have a serious lack of electronic countermeasures (ECM), which could be used against American equipment provided to the South Koreans.

The MIG-21 should prove comparable to the backbone of the South Korean force, the F-5E. Though a good plane, particularly when equipped with ECM, the F-5E is used by the US itself only as an "aggressor aircraft" in war games. The F-4D/E *Phantom*, the workhorse of the Vietnam War, is better than anything the North Koreans fly, but is available only in limited numbers. Both the Phantom and the F-5E have an all-weather capability. They are equally versatile as fighters or as fighter-bombers, but the North Korean planes are much less so. The MIG-21, for example, has a payload just one-eighth that of the Phantom.

More crucially the South Koreans are schooled in the US doctrine of close air support. In contrast, the North Koreans may "soften" selected tactical terrain before offensive operations, but they do not perform close air support for ground units in combat with the enemy. This would make the South Korean Air Force far more useful in the close quarters dictated by Korea's terrain. It would not, however, necessarily endanger the North Korean planes while they were on the ground because the North has an extensive system of underground shelters for its aircraft.

Besides protective cover, the North has a thick air defense network with a complete radar net and an early warning capability. In the field, the North Korean forces are accompanied by air defense regiments possessing around 9,000 antiaircraft (AA) guns of all sizes, including the Soviet-manufactured, self-propelled ZSU-57-2 with twin 57mm AA guns. Antiaircraft coverage in the corps area of operations is excellent. Guns are augmented by the handheld *Strela* missile and three SAM (surface-to-air missile) brigades with 250 SA-2 Guideline missiles. All of these weapons, as the Arabs superbly demonstrated during the early stages of the Yom Kippur War, are designed to form an interlocking network, with a type weapon for every level of flight.

On the South Korean side of the line, AA protection is more scarce. The largest weapons are the 40 Nike-Hercules launchers (140 km range). Tactically, the ground forces are hurt by the fact that only now is the US testing a high-quality, short-range, all-weather, day/night air defense gun system, the *Roland*. Thus the South Koreans have only a weak assortment of AA weapons, ranging from the outdated US M-42 40mm, self-propelled, AA system to the excellent Hawk missile. Troops have the SA-7's American-made



counterpart, the Redeye.

Analyzing North and South Korean AA systems as a whole, it can be seen that although the SA-2 is the mainstay of North Korean air defense, the real bulk of the system contains AA guns. This is to be expected because the first large-scale uses of guided missiles by ground air defense forces were not until the Vietnam and Yom Kippur Wars. In these conflicts,it was significant that the most effective means of bringing down planes was the AA gun. It should be noted that this happened after the planes had been forced closer to earth by the missiles, and only with conspicuous ammunition consumption rates. Missile expenditure, however, was also very high, and aircraft losses recorded must be balanced against the large number of missiles fired.

The use of American systems in the Yom Kippur conflict was highlighted by the performance of the American *Hawk* missile system, which is extremely accurate and is present in South Korea's force structure. The basic *Hawk* possessed by the South Koreans is relatively costly to operate and maintain, so in 1977 Seoul began converting to the improved *Hawk* configuration.

**Use of Terrain.** At this point in the study, all major assets of the ground and air orders of battle have been presented and analyzed. The North has a clear advantage in armor, artillery, and air defense gun systems. Rocket forces and APCs are comparable. In airpower, the South, with its superior combat avionics and protective electronic subsystems, is marginally superior: the danger is that the North's greater numbers would ultimately prevail. Such a situation is also true of the ATGM category. South Korea, with the TOW, has an advantage in quality, but it is doubtful if there are enough of these launchers and their missiles in-country to offset the large numbers of North Korean tanks and ATGM assets.

Superior numbers pose the major problem on the ground for the South. With the exception of artillery, where Soviet models are superior to their American opposites, South Korean equipment is generally a match for North Korea's weapons. To counter this disadvantage in numbers, the South Koreans will make full use of the terrain, appropriately studded with mines, obstacles, and fortifications. The rugged nature of the land is such that North Korean options for routes of advance are extremely limited. The Chorwon Valley is only 29 km wide; the Kaesong-Munsan approach is only 9.5 km wide.

According to Soviet and North Korean doctrine, the assigned frontage for a motorized infantry division in the attack is 10 to 16 km; for a tank division, 12 to 15 km. The width of the attack zone within these assigned areas is 4 to 8 km for infantry and 5 to 8 km for tanks. The South's smaller numbers, when deployed in the defense, are not as detrimental as raw figures would indicate. The standard textbook factor of automatically tripling the capability of a unit in the defense becomes increased still further, under circumstances like those in Korea, because the North could only commit its forces piecemeal.

The North's superiority in equipment appears sufficient to insure the necessary breakthrough. Because the South Koreans would certainly lose defensive line Alpha around 5 km below the DMZ, they would have to focus their effort on stopping the North just short of Seoul. If the South was able to keep the initial North Korean penetrations to a minimum and to contain them for 72 hours, Northern chances of breaking through thereafter would be slight. The primary threat to such a successful stand would be the North Korean dominance in armor and artillery.

**"Human Factors."** North and South Korean armed forces are noted for their rigorous approaches to discipline although the life of a North Korean soldier is the more harsh of the two. The North also has a more demanding training routine, sharpened by the length of service required of personnel: 5 years for the army and navy, and 3 to 4 years for the air force; and for South

Korea, 3 years for the navy and air force, and 2.5 years for the army and marines. Also, North Korea keeps its forces on permanent alert, which gives them more opportunities for weapons training, live-fire exercises, and general military training.

The South has a larger defense budget, but it is a smaller proportion of estimated GNP than for the North. In per capita spending on defense, the North exceeds the South by more than 2:1. The North Korean system supports the military at the expense of other sectors, which is reflected in the massive size of the armed forces.

In part, the South hopes to redress this imbalance through the experience of its personnel. Many officers and noncommissioned officers acquired combat experience in Vietnam. During the war, a South Korean force of 50,000 was deployed in two divisions. This allowed the rotation into combat and subsequent training of numerous leadership personnel. These personnel are still in the force structure and have been able to put their lessons to use.

Generally, both Koreas are well trained and highly motivated. Consequently, neither has any considerable advantage. Despite the involvement of certain South Korean military units in past political actions, there is no evidence that any sort of trend towards politicization has been given impetus. Within both armed forces, tenacious execution of assigned missions is to be expected, giving weapons systems high lethality.

**Naval Forces.** A final word must be added with respect to relative naval strengths. The less-than-complete treatment given to the maritime aspect of any conflict is because of the limited role naval forces would play. The North's fleet is significantly stronger than the South's fleet because of its 20 submarines. The South has neither submarines nor a developed anti-submarine warfare (ASW) capability.

The bulk of both forces contains assorted gun-armed patrol craft. The North has a very large fleet, many vessels of which are built locally. Quite a few are due for retirement, but the fleet is strengthened by Soviet-built *Osa* and *Komar* missile craft. South Korea's American-designed, but largely locally-built, fast patrol boats (FPBs) are modern, well armed, and very fast, but the fleet is small by comparison with the North's assets.

With the wide discrepancy in numbers, and with quality on an equal basis, it would be a matter of time before the North Koreans were able to achieve superiority at sea. At the same time, it is difficult to see such a result having any decisive impact on the outcome of a conflict between the two sides in isolation. The key to the struggle would be on the ground and in the air.

**Conclusions.** The evidence indicates that South Korea does not currently have the means to defend itself. With their present strength in key categories, the North Koreans would be able to reach Seoul in any invasion. This, of course, would virtually sound a death knell for South Korea. The additional factors of EW and NBC capabilities tip the scales even more in the North's favor. Although the two sides are roughly equal in EW assets, the Soviets could give the North Koreans the benefit of their recent NBC experience.

Long-range trends are of no comfort, because since 1970 the North has steadily increased its force levels in an arms drive which is essentially unilateral and is independent of South Korean actions. This drive has been highlighted by the North's continued attempts to design and produce its own armor, artillery, and self-propelled guns. Continued expansion of armor forces, together with the introduction of more sophisticated Soviet weapons like those already present in Arab armies, would present an even more serious threat than the one already outlined.

As far as South Korean force levels are concerned, improvement would certainly not tip the balance because it has already been pointed out that the South Koreans are inferior to the North Koreans in key categories. Nevertheless, American policy has not allowed the South to obtain the more desirable or potent items it needs.[6] To blame the situation solely on the US would be naive, because South Korea has obviously made policy decisions which have properly treated the military as but one important sector among many. In contrast, North Korea has essentially a war economy, nearly totally dedicated to supporting armed forces far in excess of any defensive need. Why the North should have chosen to do this is beyond the scope of this study, but the results in the field have been impressive and have left the South in a dangerous position, vulnerable to an attack.

1. Interview with LTG Edward Meyer, US Army Chief of Plans and Operations, on ABC Special, *The American Army: 'A Shocking State of Readiness,'* KITV, Honolulu, 1 May 1978.
2. Russell Spurr, *The Hollingsworth Line*, **FAR EASTERN ECONOMIC REVIEW**, 27 February 1976, pages 26-28.
3. Given the South Korean need for a reconnaissance vehicle with heavier armament, it is significant that Seoul has recently negotiated the purchase of a number of American M-551 Sheridans with their 152mm gun/missile launchers.
4. Reliable sources feel that these forces may actually consist of two mechanized and two motorized divisions.
5. US ATGMs are "second generation"; i.e., the gunner must track only the target. The North Koreans have "first generation" systems which require the gunner visually to track both the missile and the target throughout the firing sequence.
6. This policy may be changing, because on 29 April 1981 the US promised to give South Korea more sophisticated arms and considerable military-related economic concessions in an effort to build East Asian defenses. Equipment offered includes the F-16 fighter, one of the world's best.

by James C. Mellen

# I am an all-source analyst

I am an all-source analyst. I understand the capabilities and limitations of HUMINT, IMINT, EMINT, RADINT, COMINT, ELINT, ground and aerial platforms of all services and nations. I can interpret broad plans and orders to enable responsive and timely tasking of these assets. I can keep track of every EEI, OIR, and every tasking, and trade them off against each report so as not to duplicate the tasks unnecessarily. I can cancel tasks when the information is obtained, and can renew the task when the data is old. I understand propagation limitations and line of sight restrictions caused by terrain masking of all types of sensors. ☐ I know tactics, understand the enemy organization, his likes and dislikes, and can anticipate what important data is necessary. I can interpret data to determine significant events from information arriving into my automated system. I know the best ways to confirm enemy activity and can initiate appropriate tasking and issue necessary warnings and estimates to those who need them. I understand terrain and weather impacts on tactics, and can predict, with the aid of my machine, where the enemy is from and where he is now located. I've read up on his capabilities for fire and maneuver, and can predict those areas where it is dangerous to be. I know what data is most useful to those involved in sorties against him. Because I understand his TO&E, his equipment capabilities, and limitations, I can relate the proper OPSEC, COMSEC, and ELSEC requirements. ☐ I can draft resource tasking messages and respond to active jamming tasks without delaying the control aspects; I can evaluate the collection and jamming missions and issue summary reports. I can capitalize on the capabilities of my resources to respond to plans, orders, and fragmentary orders, as well as indications I perceive. My vast experience helps me to know what are obvious deception operations, and for those not so obvious, I know how to immediately retask resources to confirm deception. Understanding cover and deception aids my ability to support the commander's OPSEC efforts. ☐ I know what are the most important ongoing actions and can divide my time and use my assets accordingly. If my automated system fails, I can perform my job manually, but slower. I know what the staff needs, and I can provide it quickly. I can present briefing data through my automated graphics display or in person. I can do all of this with security aspects of protecting the source foremost in my mind. I can perform in any weather or climate, in my environmental or NBC protective equipment. I am a tasker, manager, collector, evaluator, correlator, critical node analyst, overall multi-discipline analyst, and reporter. What I do not know is

MY MOS.

# bar code labels for classified documents

by James M. Ganz

Could the Army use the same system to control classified documents as the one used to manage food in your neighborhood supermarket? Why not?

This question, or one like it, was posed to the Army Electronics Research and Development Command (ERADCOM) nearly a year ago. Since that time, the command's staff has been planning a major test of this new technology in the document-control world. ERADCOM's Signals Warfare Laboratory (SWL), Vint Hill Farms Station, Warrenton, Virginia, will be the chosen site for the pilot test program.

Classified holdings in two of SWL's divisions will be converted to the bar code label system during the first 6-month test period. The divisions' documents will be dually controlled, using both the conventional manual method and the bar code labels. After the test period, an evaluation of time and motion studies and economic analysis will be made to determine the system's adaptability for general use throughout ERADCOM and then the Army.

The equipment to be used consists of simple alphanumeric high-density code 3-of-9 adhesive tags manufactured by Markem Corporation, Keene, New Hampshire, and the MSI model 88 bar code label scanner. The scanner has 48,000 bytes of memory and communicates with the computer over telephone lines through the use of a built-in acoustic coupler.

SWL has used bar code labels before to keep track of equipment and property. In fact, it was their ability to separately and distinctly identify property-book items that earned them a satisfactory grade and a laudatory letter from Army Materiel Development and Readiness Command evaluators in 1980.

Conventional inventories without bar code labels were always cumbersome. A lot of time was spent identifying and verifying every item. Unless a positive step was taken, some pieces may have been counted more than once, and others not at all.

Using bar code labels eliminated all this. Because all the research work and cross-referencing was done once up front, a faster and more accurate inventory resulted. Each piece of equipment or furniture had its own label number. This feature made reconciliation very easy, because controlling information linking the label number to a particular custodian, organizational element, or room could be added to the data base. The end result was a machine-generated listing of overages or shortages that greatly reduced the time normally spent in reconciling and typing forms.

All this led to adopting the data base and labels for control of classified documents at SWL. Today, both property accountability and document control systems are semiautomatic. Most inventories and forms are prepared manually, while the computer is used for other transactions and data manipulation. Soon, both will be fully automated. When a classified document is received in the laboratory, a DA Form 3964,

Classified Document Accountability Record, is prepared and an entry made on DA Form 455, Mail and Document Register. Another entry is made on the data base, and the document is ready to go from the top secret and secret control officer to the division custodian. A bar code label is affixed to the document, and the label number is added to the base as a means of cross-referencing to other control items.

The individuality of items with bar code label numbers is helpful when controlling classified documents. Under the old control system, if a document consisted of a letter, with two endorsements and three enclosures, all classified, the entire package (document) was assigned one control number. With the labels, there are six numbers cross-referenced to the one current control number. If there are multiple copies of a document, then each copy, including each item, has a separate number.

To conduct an inventory under the old system, the custodian and a witnessing official had to locate each document, physically handle it, review it for downgrading or declassification, and verify that the document in hand was indeed the same as that named on the receipt, and that all controlling data was accurate. Then, the custodian provided a listing of findings to the top secret and secret control officer and a mutual reconciliation took place.

Using the new system, the inventory is accomplished by reading the label number with the scanner. Reconciliation is performed automatically when the machine generates a shortage/overage report.

During the pilot program at SWL, emphasis is being given to enhancing the inventory process, with particular attention on verification and reconciliation. It is anticipated that a 40 percent savings in manpower can be realized in just these two areas, and the need for a witnessing official can be entirely eliminated.

Figure 1 shows the items included in the SWL classified documents control data base. Listings (reports) can be generated for any item on the left side of the table. With bar code labels, two additional items can be added: the bar code label number, and discrepancies (over/short). There is also room in the data base for name, account number, building, division, branch, room, safe number, and drawer.

To keep documents from being illegally reproduced, the labels will be color coded according to security classification: red for secret, yellow for top secret, etc. If a document is reproduced without approval, it will have a black label, and thus will be easily detected as fraudulent. On those occasions when reproduction is approved, a new color-coded label will be applied, and the necessary controls entered into the data base.

## CLASSIFIED DOCUMENTS DATA BASE

**Control number**
**Division**
**Classification**
**Date received**
**(also range of dates)**
**Status**
**(A=active,**
**I=inactive,**
**D=destroyed.)**
**Courier/Register number**
**Review/Declassify**
**Individual item (of items)**
**Number of copy (of copies)**
**Date originated**
**Description**
**Remarks**
**(Destruction/Transmission data)**

Figure 1

Figure 2 shows one application of the bar code label technology that has labor-saving potential. When a new document is received, a label can be applied. The label could then be read by the scanner and transmitted to the computer by remote terminal. The computer could query the terminal on input, and controlling data could be entered to form a permanent record. On command, the computer would provide the prescribed information to a line printer, where DA Forms 3964 and 455 would be printed. This would save the time-consuming manual preparation of these two forms.

Using bar code label technology for control of classified documents has unlimited possibilities. Although the pilot program at SWL will target on inventory enhancement and focus on the verification and reconciliation phases, an incremental plan of attack will be employed. After successful completion and adoption of each increment, another, more ambitious effort will be tested and evaluated.

It is quite possible that over the horizon there may be a whole new method of controlling classified documents in the 1980s.

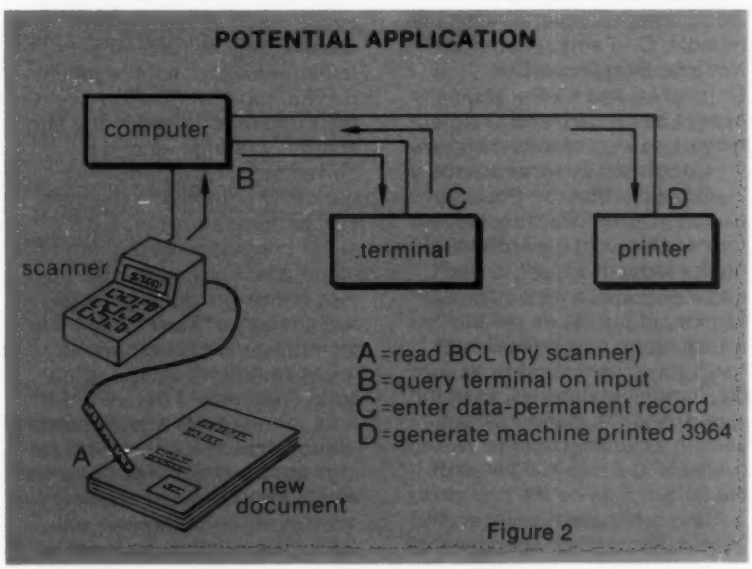



Figure 2

# what's wrong with "reliability"/

## Introduction

The first step in processing military intelligence is evaluating reports derived from various sources. Evaluation has traditionally included determining the "reliability" of the reporting source and the "accuracy" of the information. Reliability represents a percentage estimate of the source's reports which have been proven true. Accuracy refers to the content of a report, and measures the probability that the reported facts are true in light of all other available information. The importance of obtaining valid data ratings has been increased by the development of automated systems that enhance the capability to acquire, process, and utilize data ratings.

The standard rating system that has been widely used for many years by the US Army and other organizations, including NATO, indicates source reliability on a six-point numerically-coded scale. The verbal labels associated with these codes are 1) Reliability of source: A—Completely reliable, B—Usually reliable, C—Fairly reliable, D—Not usually reliable, E—Unreliable, and F—Reliability cannot be judged; and 2) Accuracy of an item of information: 1—Confirmed by other sources, 2—Probably true, 3—Possibly true, 4—Doubtfully true, 5—Improbable, and 6—Truth cannot be judged.

For example, a report from a source judged "fairly reliable" whose content is considered "probably true" would be rated C2. A detailed description of the scales, and the standards to be used in assigning ratings, is available in Army Field Manual FM 30-5.

Although these 6-point scales have been used for many years, certain basic questions are raised concerning their intrinsic meaning to raters and users of intelligence reports. For example, to what extent does each scale represent separate, non-overlapping categories? How well would different analysts agree upon the quantitative meaning suggested by each of the individual and joint ratings? In different situations, how consistent are individual analysts in the way they interpret the scales? A few previous experimental studies, and the present study, address certain aspects of these questions.

**These studies suggest that real difficulties accompany the use of the reliability and accuracy scales.**

One study[1] examined spot report ratings in an Army field exercise. Of all reports processed, only 48 percent contained ratings of source reliability and information accuracy. On the rated reports, reliability and accuracy ratings tended to be correlated. The ratings were generally confined to the high end of the scale; in fact, B2 alone comprised 74 percent of all ratings.

In follow-on work,[2] ratings assigned by officers enrolled in an intelligence course were found to differ from the school solution about 15 percent of the time for reliability and 49 percent of the time for accuracy. No ratings improvement was observed when ratings were made with the aid of a decision flow diagram (i.e., a programed sequence of simple questions) designed to reduce the complexity of the rating procedure and to guide the rater to the appropriate rating.

These studies suggest that real difficulties accompany the use of the reliability and accuracy scales. Whether these problems are due to basic inadequacies in the scales or to the inability of intelligence analysts to use them properly is a question for research. The present investigation examined the structure of the scales, with particular emphasis on a subjective quantitative interpretation of the various ratings and their combinations.

## METHOD AND RESULTS

Thirty-seven Army captains, enrolled in a Military Intelligence officers career course, participated in the study. In each of two experimental sessions, all participants were required to complete four paper-and-pencil forms, which will be referred to as Forms 1 through 4. Each form and corresponding instructions are described below. The initial session began with an introductory briefing, with participants completing Forms 1, 2, 3, and 4, in that order. Forms were distributed and collected one-at-a-time, and the order of presentation was arranged to minimize the possibility that performance on one task would influence performance on a subsequent task. In the second session, conducted exactly two weeks after the first session, participants repeated the identical procedure followed in the first session. Statistical comparisons showed responses for each participant to be highly consistent over the two sessions, and all data presented represents an average performance.

# "accuracy" rating scales??????

by Michael G. Samet

**FORM 1**

**Method.** In Form 1, participants were required to make 100 comparative judgments. Each judgment was based on the following excerpt from the instructions to participants:

> Suppose that you have two intelligence reports, one saying that camp X will be attacked and the other saying that camp Y will be attacked. The reports differ only in their respective ratings for the reliability of the report's source and the accuracy of the report's information. On the basis of this information alone, your task is to decide whether it is more likely that camp X will be attacked or that camp Y will be attacked. For example, suppose that in the first problem the report that camp X will be attacked was assigned A3 and the report that camp Y will be attacked was assigned C1. On your sheet the problem would appear as follows:
>
> | Report camp X | Report camp Y |
> |---|---|
> | A3 vs. C1 | |

Participants indicated their decisions by circling the ratings of one of the two reports (either A3 or C1 in the example).

The 100 problems used all systematically derived combinations of reliability ratings A through E and accuracy ratings 1 through 5. One joint rating had a higher reliability rating, and the other had a higher accuracy rating (i.e., A2 vs B1, A2 vs C1, A2 vs D1, A2 vs E1, A3 vs B1,..., A3 vs E2, A4 vs B1,..., A4 vs E3, A5 vs B1,..., A5 vs E4, B2 vs C1,..., D5 vs E4). Each participant received the problems in a different random order, and the left-right orientation of each pair was also randomized.

**Results.** For each problem the participant decided which report's content was more likely, based on a rating of higher reliability versus higher accuracy. The percentage of decisions made according to higher accuracy was computed in each session (this number is 100 percent minus the percentage of decisions made according to higher reliability). Overall, an average of 75 percent of the decisions were made according to higher accuracy, and 25 percent were made according to higher reliability. Only one participant responded to according higher reliability on a majority of problems. To determine which of two reports was more likely to correctly predict an event, participants showed a clear and consistent preference to decide in favor of the report assigned a higher accuracy rating but lower reliability rating.

**FORM 2**

**Method.** In Form 2a, participants were given the specific reliability rating carried by a report. They were asked to estimate the conditional probability that the report carried a specific accuracy (reliability) rating. This was based on the following excerpt from the instructions to participants:

> On each problem you will be given the reliability rating carried by a report; in light of this rating, your task is to estimate the probability that the report carried a given accuracy rating. You are to state the probability as any number between 0 and 100, inclusive. This number can be thought of as your estimate of the number of chances in 100 that, given the known reliability rating, the report carried the given accuracy rating.

A sample problem is the following: Given that the reliability of the source was rated B, what is the probability that the accuracy of the information was rated 4?...A report has come through whose source reliability was rated B. The information accuracy was also rated, but the rating has been lost in the processing system and you do not know what it is. What is the probability that the accuracy rating was actually 4?

**Overall, an average of 75 percent of the decisions were made according to higher accuracy, and 25 percent were made according to higher reliability.**

In Form 2b, reliability and accuracy were interchanged, and the corresponding question was: "Given that the accuracy of the information was rated 4, what is the probability that the reliability of the source was rated B?"

Each of the six reliability ratings (A thru F) was paired with each of the six accuracy ratings (1 thru 6). This generated 36 problems for Forms 2A and 2B. For each participant, the 36 pairs of ratings were put in a different order.

**Results.** Ten of the 37 participants responded as if the reliability and accuracy ratings were independent. Thus, each rating

of reliability or accuracy was considered equally likely to be observed.

The results for Form 2 are based on the remaining 27 participants. None of these participants normalized their response probabilities across a given reliability or accuracy rating. A statistical analysis showed that participants, in assigning probabilities, were not affected by the conditional probability orientation. That is, for any reliability (R) and accuracy (A) rating, the conditional probability of A given R.

**Suppose a report comes through that your camp will be attacked tomorrow and the report has been rated A1. What would you say is the probability, or number of chances in 100, that your camp will be attacked tomorrow?**

Data were pooled over participants and orientation and were then appropriately normalized to obtain mean conditional probability values. The normalized means are shown in table 1 (note that the sum of probabilities in any row or column is 1), which is symmetric and can be read on the basis of the rows or columns. For example, the mean conditional probability for reliability rating C given an accuracy rating of 2 is .21; and the mean conditional probability for accuracy rating of 2 given a reliability rating of C is also .21. The pattern of interaction between reliability and accuracy (or vice versa) becomes clear in noting that the highest normalized mean probability in each row or column of the table is located in the diagonal position. Furthermore, in departing from the diagonal within any row or column, the means fall off monotonically. For example, if a report carried a reliability rating of C, participants considered it most likely to carry an accuracy rating of 3, and more likely to carry a rating of 2 than 1, 4 than 5, and 5 than 6.

**TABLE 1.**

Symmetric Normalized Mean Conditional Probabilities (highest probability within each row/column is circled)

| Reliability Rating | Accuracy Rating 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| A | (.27) | .23 | .18 | .11 | .08 | .07 |
| B | .24 | (.25) | .20 | .13 | .10 | .09 |
| C | .19 | .21 | (.24) | .16 | .14 | .12 |
| D | .13 | .14 | .17 | (.21) | .20 | .16 |
| E | .09 | .12 | .14 | .20 | (.25) | .20 |
| F | .08 | .10 | .12 | .18 | .21 | (.28) |

**TABLE 2.**

Mean Probabilities Assigned to Joint Ratings

| | | | | |
|---|---|---|---|---|
| A1=.96 | A2=.86 | A3=.74 | A4=.55 | A5=.38 |
| B1=.92 | B2=.81 | B3=.67 | B4=.48 | B5=.31 |
| C1=.87 | C2=.74 | C3=.60 | C4=.42 | C5=.25 |
| D1=.81 | D2=.64 | D3=.48 | D4=.32 | D5=.19 |
| E1=.75 | E2=.56 | E3=.40 | E4=.24 | E5=.14 |

**Form 3**

**Method.** In Form 3, participants were required to assign a numerical probability of an event reported under each joint rating. Reliability ratings A through E were combined with accuracy ratings 1 through 5 to create 25 joint evaluations. The following is an example:

> Suppose a report comes through that your camp will be attacked tomorrow and the report has been rated A1. What would you say is the probability, or number of chances in 100, that your camp will be attacked tomorrow?

**Results.** An analysis indicated a very high level of agreement among participants in the rank orders assumed by their assignments to the 25 joint ratings (table 2).

The average range in subject assignments was .45; the range was narrowest for A1 (.88 to 1.00) and widest for E1 (.35 to 1.00). This test revealed a pattern attaching greater weight to the accuracy rating. A decrease in two levels of reliability rating has about the same effect as a decrease in one level of accuracy rating.

Forms 1 and 2 were compared to determine the consistency of

each participant. Suppose that in Form 2 the participant assigned x and y to the events reported under two different joint ratings, RA an R'A', respectively. If he decided, in Form 1, that the event reported under RA was more likely than that reported under R'A', then his choice response was considered as one of the following: (1) consistent, if x is greater than y; (2) ambiguous, if x=y; (3) inconsistent, if x is less than y. Pooling responses over all participants, 65.3 percent were consistent, 11.5 percent were ambiguous, and 23.2 percent were inconsistent. The level of disagreement, between participants' numerical assignments and their comparisons was high.

**Method.** In Form 4 participants were required to estimate a numerical probability of an event reported under each reliability rating (from A thru E) or accuracy rating (from 1 thru 5) appearing by itself. The following is an example:

> Suppose a report has come through that your camp will be attacked tomorrow and the reliability of the source was rated A but no rating was made for the accuracy of the information. What would you say is the probability, or number of chances in 100, that the camp will be attacked tomorrow?

**A decrease in two levels of reliability rating has about the same effect as a decrease in one level of accuracy rating.**

**Results.** Assignments were consolidated, and the mean, range, and standard deviation for each rating are given for reliability and for accuracy in table 3. The mean probabilities assigned to the scale values described a significant trend for both reliability and accuracy. With the exception of the highest rating (1), the accuracy ratings were assigned in multiples of .20.

**TABLE 3.**

Mean, Range, and Standard Deviation for Probabilities Assigned to Individual Ratings

| Rating | Verbal Descriptor | Mean | Range | Standard Deviation |
|---|---|---|---|---|
| **Reliability** | | | | |
| A | Completely reliable | .86 | .65-.99 | .11 |
| B | Usually reliable | .73 | .55-.90 | .12 |
| C | Fairly reliable | .57 | .40-.80 | .13 |
| D | Not usually reliable | .36 | .15-.70 | .15 |
| E | Unreliable | .18 | .05-.53 | .15 |
| **Accuracy** | | | | |
| 1 | Confirmed by other sources | .93 | .70-1.00 | .09 |
| 2 | Probably true | .79 | .53-.90 | .10 |
| 3 | Possibly true | .61 | .40-.80 | .14 |
| 4 | Doubtfully true | .38 | .15-.65 | .16 |
| 5 | Improbable | .21 | .03-.53 | .16 |

In general, as the degree of reliability/accuracy declined, the range length and standard deviation for each rating increased, indicating that subject's numerical interpretations of the ratings became more divergent.

## DISCUSSION AND CONCLUSIONS

The results of these exercises indicated difficulties in the interpretation of the qualitative scales used to rate source reliability and information accuracy. One obvious problem is the wide difference of opinion suggested by each rating. For example, assigned probabilities for both "fairly reliable" and "probably true" ranged from .40 to .80. However, the results of the correlational analysis for Form 3 data indicated agreement among the participants. Although this agreement on the rank order of one rating relative to another is encouraging, the disagreement on the numerical meaning of each rating raises doubts about the effectiveness of the qualitative rating scales.

The rating scales lack sufficient sensitivity for expressing the degree of reliability and accuracy. The results of Form 4 indicated the participants were able to make a clear distinction between the five meaningful levels of each scale, suggesting that there is room for finer discrimination. The sensitivity of the scales is reduced by the availability of the ratings of "F" and "6" which allows the analyst an easy way out from making difficult evaluation.

**One obvious problem is the wide difference of opinion suggested by each rating.**

Another difficulty with the rating scales is that nearly one fourth of all response patterns on Form's 1 and 3 were inconsistent. For example, in Form 3 a subject may have assigned probabilities of .70 and .60 to reports carrying ratings of B3 and D2, respectively. Yet in Form 1, he may have considered an event more likely if reported under D2 rather than under B3. A further analysis showed that the greater a subject's tendency to use only one dimension (reliability or accuracy) in deciding which rated reports were likely to be true (Form 1), the fewer the number of inconsistent response patterns for the subject.

A further problem in the reliability and accuracy scales is that many analysts don't accept that the two ratings are independent of each other; the higher a report's reliability rating, the higher the accuracy rating expected, and vice versa. This trend is reasonable because when no other information is available, the expected accuracy of a given report is equivalent to

**Another difficulty with the rating scales is that nearly one-fourth of all response patterns on Forms 1 and 3 were inconsistent.**

the reliability of its source. The dominance of a report's accuracy rating over its reliability rating is not surprising in the findings on Forms 1 and 3. In summary, the assumption that reliability and accuracy ratings can either be made or perceived independently cannot be defended on logical or empirical grounds.

The conclusion justified by this experiment and other research [1,2,3] is that the ambiguity and insensitivity of the reliability and accuracy scales are functions of their qualitative nature and structure. An effort should be made to design and validate a new, more effective system to communicate evaluations of intelligence data. The findings suggest that the two-dimensional evaluation be replaced by a single evaluation in which an intelligence report would be rated by its liklihood of being true. A specific rating could be based upon integration of all available information: the reliability of the source, confirming and nonconfirming reports from the same and other sources, the situation, etc. This rating could be associated with the report and used in subsequent data communication and processing. This scheme does not decrease the benefit of measuring a source's reliability and its continuous revision according to accumulated evidence. This reliability rating would be available to serve in data collection management. In the absence of any other information, the analyst/system could rely upon the latest reliability index as a probability estimate for a given report being true.It might be desirable to maintain and use separate reliability ratings for different categories of information furnished by the same source.

The use of a well-defined quantitative scale should reduce ambiguity and individual differences in communicating and interpreting intelligence evaluations. When numbers instead of words are used in probability statements, differences in interpretation due to context[4] will be less likely to occur.Inconsistencies observed in this experiment would not occur if comparisons between reports are made on the basis of two larger or smaller comparable numbers. A quantitative rating system would be compatible with manual and automated procedures, and equally comprehensible across language barriers. Numbers can also be input into computerized models designed to process probabilistic information.[5] Preliminary research has shown that a quantitative scale can be used to rate photointerpreter reports,[6] and that it can be accepted by intelligence analysts.[7]

The first step in designing a rating system would be to determine which form might best be expressed. Two forms that show promise are a probability scale (e.g., 0.00 to 1.00 or 0 percent to 100 percent) and some kind of odds scale. Another possibility worth investigating is whether the addition of fixed verbal annotations associated with certain values on the numerical scale can be benefi-

**An effort should be made to design and validate a new, more effective system to communicate evaluations of intelligence data.**

cial. Extensive laboratory and field evaluations of any new rating system devised, including comparisons with the old system, would be desirable before it could be accepted and implemented.


### ACKNOWLEDGMENTS

This work was supported by the U.S. Army Research Institute for the Behavioral and Social Sciences (ARI) (Alexandria, Virginia). The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of ARI, the United States Army, or the Department of Defense.

**Footnotes**


1. Baker, J.D., McKendry, J.M., and Mace, D.J. **Certitude Judgements in an Operational Environment.** Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, Technical Research Note 200, November 1968.
2. Baker, J.D. and Mace, D.J. **Ceriitude Judgements Revisited.** Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, unpublished manuscript, 1973.
3. Meeland, T. and Rhyne, R.F. **A Confidence Scale for Intelligence Reports: An Application of Magnitude Estimation Scaling.** Menlo Park, CA: Stanford Research Institute, Technical Note 4923-31, June 1967.
4. Johnson, E.M. **Numerical Encoding of Qualitative Expressions of Uncertainty.** Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, Technical Paper 250, December 1973.
5. Johnson, E.M., Cavanagh, R.C., Spooner, R.L., and Samet, M.G. *Utilization of Reliability Measures in Bayesian Inference: Models and Human Performance.* ***IEEE Transactions on Reliability,*** 1973, R-22, 176-183.
6. Samet, M.G. **Checker Confidence Statements As Affected by Performance of Initial Image Interpreter.** Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences, Technical Research Note 214, September 1969.
7. Kelly, C.W. and Peterson, C.R. **Probability Estimates and Probabilistic Procedures in Current-Intelligence Analysis.** Gaithersberg, MD: International Business Machines Corporation, Report 71-5047, January 1971.


**Correction:**

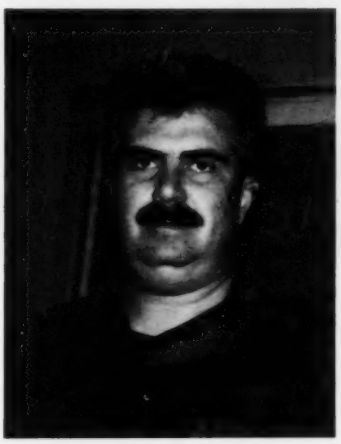
The following correction should be noted for July-September 1981 issue:

Page 55: In the first chart from the article 'I Didn't Know That' 50 Baud should read 50K Baud

# USAICS notes

On October 8, 1981, Brigadier General James A. Teal turned over the command of USAICS to Brigadier General Roy M. Strom.

Prior to the change-of-command ceremony, Strom was promoted from Colonel to Brigadier General.



Sergeant First Class Richard A. Henson recently scored 100% on his annual Skill Qualification Test. SFC Henson, an 05G4H, is currently assigned as a Signal Security Instructor in the Department of Human Intelligence (DHI).

Sergeant Henson has over sixteen years active military service. Prior to his arrival at Fort Huachuca he was a Technical Publications Writer/Editor at USAISD, Fort Devens, Massachusetts. SFC Henson, a native of New Hampshire, has an Associates of Science degree in Law Enforcement and is currently working on a Bachelor of Arts degree in Management.

# USAISD notes

## USAISD RE-ACCREDITED

The President of the New England Association of Schools and Colleges (NEASC) has announced the continued accreditation of USAISD through December 1986. NEASC is the agency authorized by the U.S. Department of Education and the Council on Post-secondary Accreditation (COPA) to accredit schools and colleges in the New England States.

Initially accredited by NEASC for a five-year term in May 1976 as a post-secondary, nondegree granting career institution, USAISD underwent reevaluation by a visiting committee representing NEASC, April 13-15, 1981.

The accreditation process involved appraisal by educators using qualitative standards established by the Commission on Vocational, Technical, Career Institutions, NEASC. Accredited status certifies that an institution conforms to those standards and is meeting its objectives. Accreditation also indicates that the purpose of an institution is appropriate for its type, and its programs, faculty, students, facilities, and resources are adequate to carry out its purpose. USAISD has met those requirements.

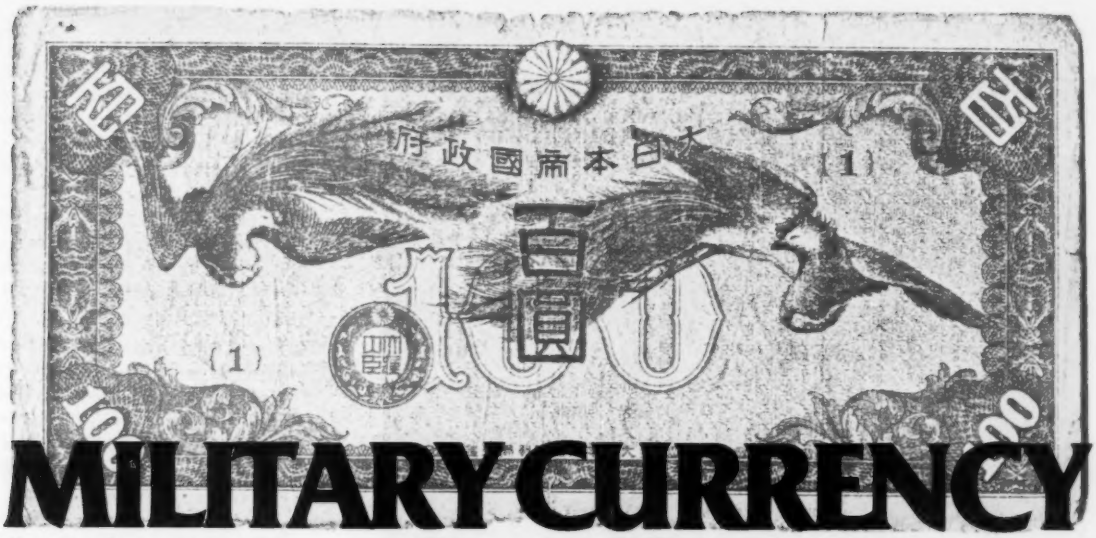
For USAISD students, accreditation means that the value and quality of their military training has been recognized by civilian educators. As a result, it may be possible for graduates of USAISD courses to obtain undergraduate or technical school credits for the training they have received. Granting of college credit hours is determined solely by the receiving institution.

## SHORT NEW USAISD COMMANDER

On October 30, 1981 the United States Army Intelligence School, Devens (USAISD), welcomed Colonel Joseph F. Short as its new commander. Short took the command from Col Stanley G. Kozlowski after a Change of Commander/Retirement ceremony at 10 a. m. on Roger Field, Fort Devens.

Short comes to USAISD from Arlington Hall Station, Va, where he was assigned as Project Manager at Headquarters, U.S. Army Intelligence Command. A native of Pawtucket, R I, Short entered active duty in November, 1956, and received an ROTC commission and a BS in business administration from the University of Rhode Island. He also holds a Masters of Education degree from Fitchburg State College.

Besides serving several tours in the United States, Short has also served in Japan, Belgium, Great Britain, Korea, and Vietnam. He has served as Commander, Vint Hall Farms Station, Va, Commander of the 226th ASA Operations Company, Korea, Assistant Chief of Staff at Headquarters, U.S. Army Security Agency, and as Staff Planner, Joint Chiefs of Staff, the Pentagon in his 25 years of service. He has attended the U.S. Army Command and General Staff College and the British War College.




# MILITARY CURRENCY in international law

by Richard A. Banyai

Military currency is a special means of payment sanctioned by international law and issued by a military power or belligerent occupant for use in an occupied territory. Generally, the right of a belligerent to occupy and govern the territory of the enemy and issue currency therein is one of the incidents of war and flows directly from the right to conquer. This is established in international law.*

Military currency is fiat money—money printed and issued by order of the government with no gold or silver backing or reserves. It may not even represent a promise to pay. The Allied Military Mark currency used in occupied Germany (1944-48)[1] and the German Reichskreditkassen Reichsmark currency used by the German military in the various German-occupied areas of Europe (1940-44)[2] are examples of this. Also, it is often printed in the monetary unit of the territory to be occupied; for example, the Japanese military currency denominated in yuan for use in China (1938-40), denominated in dollars for use in Malaya-Singapore (1941-45), and denominated in pesos for use in the Philippines (1941-45).[3] There is ample case precedent for the issue of military currency.†

The issuing power may not accept any responsibility for the military currency that it issues. Usually the occupying power attempts to force responsibility upon the occupied territory for the continued acceptance and exchange of the military currency issued during the occupation. This saddles the occupied area with part of the occupation costs represented by expenditures of military currency.[4]

In an occupied territory, there are three types of currency which an occupant can use for general means of payment or from which one may be selected as a means of payment: local currency, belligerent occupant's own currency, and military occupation currency.[5]

Twenty yen military currency issued in Japan and Okinawa in 1945 by the US military authority.

### Local Currency

Local currency is the occupied territory's own money used by the belligerent occupant within the captured country (e.g., German Reichsmarks in Germany or

*Dooley v. US, 182 US 222 (1901); US v. Rice, 4 Wheat (16 US) 246 (1819); the Venice Case, 2 Wall (69 US) 259(1864); Ochoa v. Hernandez y Morales, 230 US 139, 154 (1913); New Orleans v. The Steamship Co., 20 Wall (87 US) 387, 393-94 (1874).

†Thorington v. Smith, 8 Wall (75 US) 1, 11 (1868); Mechanics and Traders Bank v. Union Bank, 22 Wall (89 US) 293-96 (1874); Haw Pia v. China Banking Corporation, 80 Philippine Supreme Court Reports 604 (1948).

Two shillings/six pence military currency issued in North Africa and Greece in 1943-1945 by the British military authority.

Japanese yen in Japan), or which has become legal tender after the occupation has begun but not as the result of any decision made by the occupying power.

Under article 43 of the Hague Regulations, the requirements of public order and respect for laws in force in the occupied territory require the belligerent occupant to maintain local currency as circulating means of payment and legal tender, if possible.[6,7]

The occupying power has the duty to allow the central bank of the occupied territory to operate and fulfill its financial responsibilities and functions. This duty ends only when the local currency ceases to be legal tender or is no longer issued. When the central bank cannot, or will not, adapt its currency policy to the new situation, the occupant may take control and make the necessary policy changes.[8]

**Belligerent Occupant's Own Currency**

The belligerent occupant's own currency is that which is legal tender in the occupant's country.

The right to introduce the occupant's own currency into the occupied territory (e.g., US dollars circulating in North Africa (1942) and Sicily (1943)[9]) can be deduced from article 43 of the Hague Regulations, noted above, and from article 52 of the Hague Regulations which allows for payments to be made in the occupant's own currency. Article 52, paragraph 3, states:

> "Contributions in kind shall, as far as possible, be paid for in cash; if not, a receipt shall be given and the payment of the amount due shall be made as soon as possible."[10]

This permits the occupant to use receipts to the bearer, and these may turn into means of payment, or military currency.

The occupant has no right to force the acceptance of its own currency for use between a private creditor and a private debtor. The occupant's own currency supplements the local currency.[11]

**Military Occupation Currency**

The Military occupation currency is a means of payment which the belligerent occupant introduces into the occupied territory and which is different from both the occupant's own national currency and the currency of the occupied territory. For example, Japan issued special military currency denominated in yuan for use in occupied North China (1938-40),[12] and the US, Great Britain, France, and the USSR issued Allied Military Authority (Alliierte Militaerbehoerde) mark notes for the invasion and occupation of Germany (1944-48).[13]

Articles 49 and 52 of the Hague Regulations authorize the occupant to satisfy the needs of the occupation army and its administration with local resources. It does not give the occupant the right to issue a special occupation currency. Article 49 states:

> "If, in addition to . . . taxes . . . , the occupant levies other money contributions in the occupied territory, this shall only be for the needs of the army or of the administration of the territory in question."[14]

On the other hand, article 52, paragraph 3, noted above, certainly permits the occupant to

use receipts to the bearer which may be de facto means of payment, or military currency.[15]

The belligerent occupant has the right to issue military occupation currency if there is the danger that the occupant's own currency may fall into the hands of the enemy; for example, in 1942 the US Military Governor of the US Territory of Hawaii authorized a special "HAWAII" overprint on US currency circulating in the Hawaiian Islands to prevent their use by the Japanese in case the currency was acquired by them.[16]

Military currency can be issued if there is the danger that the occupant's own currency may flow back to the country of origin and create an inflationary climate; for example, the Japanese military authority in China issued regular Bank of Japan

Fifty Reichsmark military currency first issued in Poland in 1939 by the German military authority and subsequently issued in the other German-occupied areas of Europe, 1940-1944.

One thousand dollars military currency issued in Malaya-Singapore in 1941 by the Japanese military authority.

yen notes overprinted "For Military Use Only" (1937-38) because previous issues of this currency without overprints flowed back to Japan and created a price inflation.[17]

Military currency can be issued if the belligerent occupant's military administration cannot satisfy its needs by using the local currency, or does not have an adequate amount of the local currency, or has difficulties in obtaining sufficient amounts of local currency, or has reasonable doubts whether it will have at its disposal a sufficient amount of currency.[18]

Once the belligerent occupant has decided to issue military occupation currency, it must provide a coverage for the currency. Valid coverage would consist of the local currency, goods and securities, and loan and credit operations of a commercial character. Coverage is not required in two cases: 1) when the belligerent occupant accepts the obligation to exchange the occupation currency for its own currency or for the local currency of the occupied territory; or 2) when the issue does not exceed the sum necessary for the payment of taxes and other imposts which the occupant is authorized to impose on the inhabitants of the occupied territory. The assumption in the second case is that the occupation currency will return, by way of taxes and imposts, to the occupying power. Also, the occupant must provide an adequate accounting system so that the total amount of military occupation currency printed and issued is known.[19,20,21,22]

Fifty mark Allied military currency issued in 1944 for the invasion and subsequent occupation of Germany by the US, Great Britain, France, and the USSR.

One thousand korun military currency issued in "liberated" Czechoslovakia in 1944 by the Russian military authority.

The use of military currencies in wartime has been an established practice since World War I and especially during World War II. Perhaps during the next large-scale military conflict—World War III—military currencies may be replaced by credit cards or electronic transfer accounts at the local banks or post offices in the occupied territory.

**FOOTNOTES**

1. Raymond S. Toy, **World War II Allied Military Currency** (2nd edition; El Cajon, California, 1965), pages 20-22.
2. Raymond S. Toy and Bob Meyer, **World War II Axis Military Currency** (El Cajon, California, 1967), pages 8-10.
3. Ibid., pages 74-90.
4. Richard A. Lester, **International Aspects of Wartime Monetary Experience** (Essays in International Finance, No. 3, August 1944, Princeton University Press), pages 1-10.
5. **US Army Manual, FM 27-10, The Law of Land Warfare,** pages 157-158.
6. Ernst Feilchenfeld, **The International Economic Law of Belligerent Occupation** (Carnegie Endowment for International Peace, Washington, DC, 1942), page x.
7. Krysztof Skubiszewski, *"Currency in Occupied Territory and the Law of War,"* **Jahrbuch fur Internationale Recht** (Gottingen, West Germany, 1961), page 162.
8. Ibid., pages 165-167.
9. Toy, **World War II Allied Military Currency,** page 15.
10. Feilchenfeld, **The International Economic Law of Belligerent Occupation,** page xi.
11. Skubiszewski, *"Currency in Occupied Territory and the Law of War,"* page 168.
12. Toy and Meyer, **World War II Axis Military Currency,** pages 77-78.
13. James Rutlader, **Allied Military Currency** (Kansas City, Missouri, 1968), pages 36-38.
14. Feilchenfeld, **The International Economic Law of Belligerent Occupation,** page xi.
15. Skubiszewski, *"Currency in Occupied Territory and the Law of War,"* pages 174-175.
16. Rutlader, **Allied Military Currency,** pages 26-27.
17. Toy and Meyer, **World War II Axis Military Currency,** pages 75-76.
18. Feilchenfeld, **The International Economic Law of Belligerent Occupation,** pages 70-83.
19. US Senate, 80th Congress (1st Session, June 1947), **Occupation Currency Transactions,** pages 72-94.
20. Arthur Nussbaum, **Money in the Law: National and International** (Foundation Press, New York, 1950), pages 497-498.
21. F. A. Mann, **Money in Public International Law** (Leyden, Netherlands, 1958), page 96.
22. Skubiszewski, *"Currency in Occupied Territory and the Law of War,"* page 181.

# officer's notes

by LTC James I. Dinniman

**ACSIGRAM's New Service**

MI Branch has started a new service. Projected assignments and school openings are announced in the weekly DA ACSIGRAM. The purpose of this service is to increase the dialogue between officers qualifying for specific assignments and their assignment officers, and to assist commanders in discussing career development possibilities with their officers.

**Officer Record Brief Changes**

Specialty Codes (SC) are now entered on the ORB in numerical order. The lower numbered SC appears in the block title—Primary SSI/MOS, and the higher numbered SC in the block title—secondary SSI/MOS (note that current terminology is initial/additional and is no longer primary/secondary). The initial SC is printed first in the ORB specialty block (1) and the additional specialty is printed on the second line of this block (2).

In the next example, the same officer is also trained and assigned as a 35C (Aerial Surveillance Officer). To show his qualification in Special Skill Identifier (SSI) 35C, this is added as **35A 35C**. If an MI Officer is trained and/or assigned in an additional SSI for his specialty, and it is not reflected on his ORB, he should forward this change through his MILPO to Official Records or to Combat Support Arms Division, Support Branch, (DAPC-OPF-S) 200 Stovall Street, Alexandria, VA 22332.

**Officer Assignment Preference Statements:**

USA MILPERCEN (DAPC-OPA-S) message, subject: Officer Assignment Preference Statement, dated 14 September 1981, is quoted for information:

"a. This is to announce a pending change to the use of the officer assignment preference statement and to solicit the submission of updated preference statements from OPMD managed commissioned and warrant officers.

"b. By October of this year, the capability will exist to store the following preference data items on the Officer Master File: 3 CONUS preferences, 2 overseas long tour preferences, 1 overseas short tour preference, 3 duty preferences, and the date of the last preference statement. This data will be used by the assignment managers when nominating officers for reassignment, and will be available on the officer master file data base. After the data items are input to the data base, the form will be filed in the career management file so that assignment officers will still have access to the narrative comments.

"c. OPMD managed officers are encouraged to submit an updated preference statement prior to December 1, 1981, to: HQDA, MILPERCEN, ATTN: DAPC-OP (Appropriate Branch), 200 Stovall Street, Alexandria, VA 22332. Branch Officer Symbols are: Colonels (C), Warrant Officer (W), AD (E-A), AR (E-R), FA (E-F), IN (E-I), CM (F-CM), MP (F-L), EN (F-E), AV (E-V), MI (F-M), SC (F-SC), AG (G-A), FI (G-F), OD (G-O), QM (G-Q), TC (G-T). These preferences will be input into the OMF beginning January, 1982. Although submission is not required, it is encouraged (AR 614-100) for officers:

1) Approximately 12 months prior to completion of an overseas tour.

2) Approximately 1 year after reporting to a CONUS station.

3) Within 60 days prior to beginning a course of instruction at a CONUS PCS service school, a civilian institute, or training with industry.

4) or desiring to change their preference."

Example: Officer with SCs 36/35

| Specialty/MOS Data | | | |
|---|---|---|---|
| PRIMARY SSI/MOS | 35A | SECONDARY SSI/MOS | 36A |
| ADDITIONAL SSI/MOS | | | |
| ASI DATA | | | |
| SPECIALTIES | CI/SIG SCTY/HUMINTELL (1) | | |
| | MILITARY INTELLIGENCE (2) | | |
| PREVIOUS DESIGNATED SPEC | | | |

| Specialty/MOS Data | | | |
|---|---|---|---|
| PRIMARY SSI/MOS | 35A 35C | SECONDARY SSI/MOS | 36A |
| ADDITIONAL SSI/MOS | | | |
| ASI DATA | | | |
| SPECIALTIES | CI/SIG SCTY/HUMINTELL | | |
| | MILITARY INTELLIGENCE | | |
| PREVIOUS DESIGNATED SPEC | | | |

# enlisted notes

### NCO Call

The videotape, NCO Call 1, subtitled The Army Reports #72, should now be at your Training Aids Service Centers (TASCs).

In this presentation, General E. C. Meyer, US Army Chief of Staff, talks about trends in non-commissioned officer's strength, discipline, individual and unit training, physical fitness, and education and professionalism.

Sergeant Major of the Army (SMA) William Connelly; SFC Charles Moore, Ft Monroe; SFC Jackie Woodfork, Ft Ord; and SFC Arthur Brighton, US Army Reserve, also participated in the discussion.

This videotape, from the Army Chief of Staff, serves as a personalized link from the Chief of Staff to the individual soldier.

Copies of this videotape are available and arrangements should be made through the commander to view them.

### ROTC ACTIVE DUTY SCHOLARSHIPS

Soldiers who've been thinking about college, but who may have been wondering how they might bankroll the venture, can cast their eyes towards an ROTC Scholarship as a possible solution.

Army ROTC has reserved 100 scholarships for active duty enlisted soldiers. These cover tuition, textbooks, laboratory fees, and certain other education expenses. For example, if one college major requires using a calculator or a slide rule, the Army will buy one or the other.

The Army will also pay scholarship winners $100 a month, up to $1,000 for each academic year, in tax-free subsistence allowance. Cadets also get paid for the six-week Advanced Camp, which they must attend in the summer between their junior and senior years.

Scholarship winners can also use any G. I. Bill or Veterans Educational Assistance Program (VEAP) benefits they may have earned while on active duty. The nearest Veterans Administrative Regional Officer can determine eligibility.

Last year the Army expanded the active duty scholarship program to give more soldiers the chance to apply. There is a new three-year scholarship, along with the two-year award.

In addition, some rule changes have extended the age limit by giving soldiers credit for active service.

For example, the old rules said applicants had to be younger than 25 on June 30 of the year in which they would be commissioned. Under the new rule, the maximum age is now younger than 29 on June 30 of the commissioning year.

This means that soldiers can count up to four years of active duty. Three years active duty extends the age limit to under 28; two years extends it to under 27, etc. This gives soldiers more time to earn credits so they can apply for the scholarships.

To apply for ROTC Active Duty Scholarships, soldiers must:

- ☐ be U. S. citizens;
- ☐ be at least 17 years old before the scholarship becomes effective;
- ☐ have served at least one year on active duty;
- ☐ have been accepted for enrollment by a college or university that offers ROTC (or the applicant must be able to make arrangements to attend ROTC classes at a nearby school which does);
- ☐ have a score of at least 115 on the General Technical (GT) Aptitude Test;
- ☐ have a satisfactory National Agency check;
- ☐ have kept a "C" average in college work;
- ☐ have two years of college credit for a two-year scholarship, or one year of college credit for a three-year scholarship;
- ☐ be recommended for the scholarship by their commanders.

Soldiers will be discharged from active duty to enter college. Once their scholarships are in effect, they will be Army ROTC cadets.

Individuals can major in any area that leads to a bachelor's degree except theology. They can take part in any extracurricular activity which doesn't interfere with military science requirements. Scholarship cadets will receive commissions as regular Army or Army Reserve second lieutenants after completing all requirements and graduating. They must then serve four years active duty.

For applications, or for more information, interested soldiers should write:

Army ROTC
HQ, TRADOC
ATTN: ATRO-CS
Fort Monroe, VA 23651

Soldiers must request scholarship applications for the '82-'83 school year between January 15 and April 15, 1982. If the request isn't received by April 15, it can't be processed for this year's cycle. Completed applications must reach HQ TRADOC postmarked no later than May 1, 1982.

### 1SG Course Update

On September 25, 1981, ceremonies were held at Fort Bliss, Texas, for the official opening of new training facilities for the Army's recently developed First Sergeants Course.

On hand for the ceremonies were SMA William Connelly and US Army Sergeants Major Academy Commandant, Colonel Joseph Ostrowidzki. Also present were Academy Command Sergeant Major Kenneth Parsons; SGM Louis Laul, Chief Instructor for the First Sergeants Course; and SGM George Drake, Chief of the First Sergeants Course Training Development

**SMA Connelly cutting the ribbon for dedication of Army's new training facility. Looking on from left to right are SGM Laul, Col. Ostrowidski, CSM Parsons, and SGM Drake.**

Branch. Additionally, some 35 other invited guests and First Sergeants Course Instructors witnessed the event.

Although the First Sergeants Course actually graduated its validation class in May of this year, this is the first building dedicated strictly for use in training First Sergeants Course students. The building (11285) is located on Biggs Army Airfield on the campus of the US Army Sergeants Major Academy.

The First Sergeants Course now comes under the operational control of the Sergeants Major Academy and is the latest addition to the Army's constantly growing NCO Education System.

The first official class began studies at the First Sergeants Course on October 5th. Some 60 senior NCOs are currently enrolled in the class.

The course is scheduled for five classes, eight weeks in duration, during calendar year 1982, and will graduate 300 students in pay grade E7 and E8.

Since the First Sergeants Course graduated its validation class, several changes have been made in the course curriculum aimed at improving the overall course content. The latest addition to the course content has been a block of instruction on communications skills.

This resulted from the expressed desires of the first graduates to have specific training on how to improve their speaking and writing abilities.

While the course is designed to cover a wide range of topics from physical training and appearance to unit administration, the most lengthy and comprehensive segment deals with Training Management. This segment includes everything from the preparation and presentation of instruction to training evaluation.

Another area of instruction considered particularly important to the potential first sergeant is Discipline and Esprit. Here the emphasis is on the practical application of the Manual of Courts-Martial as it pertains to the daily activities of the unit.

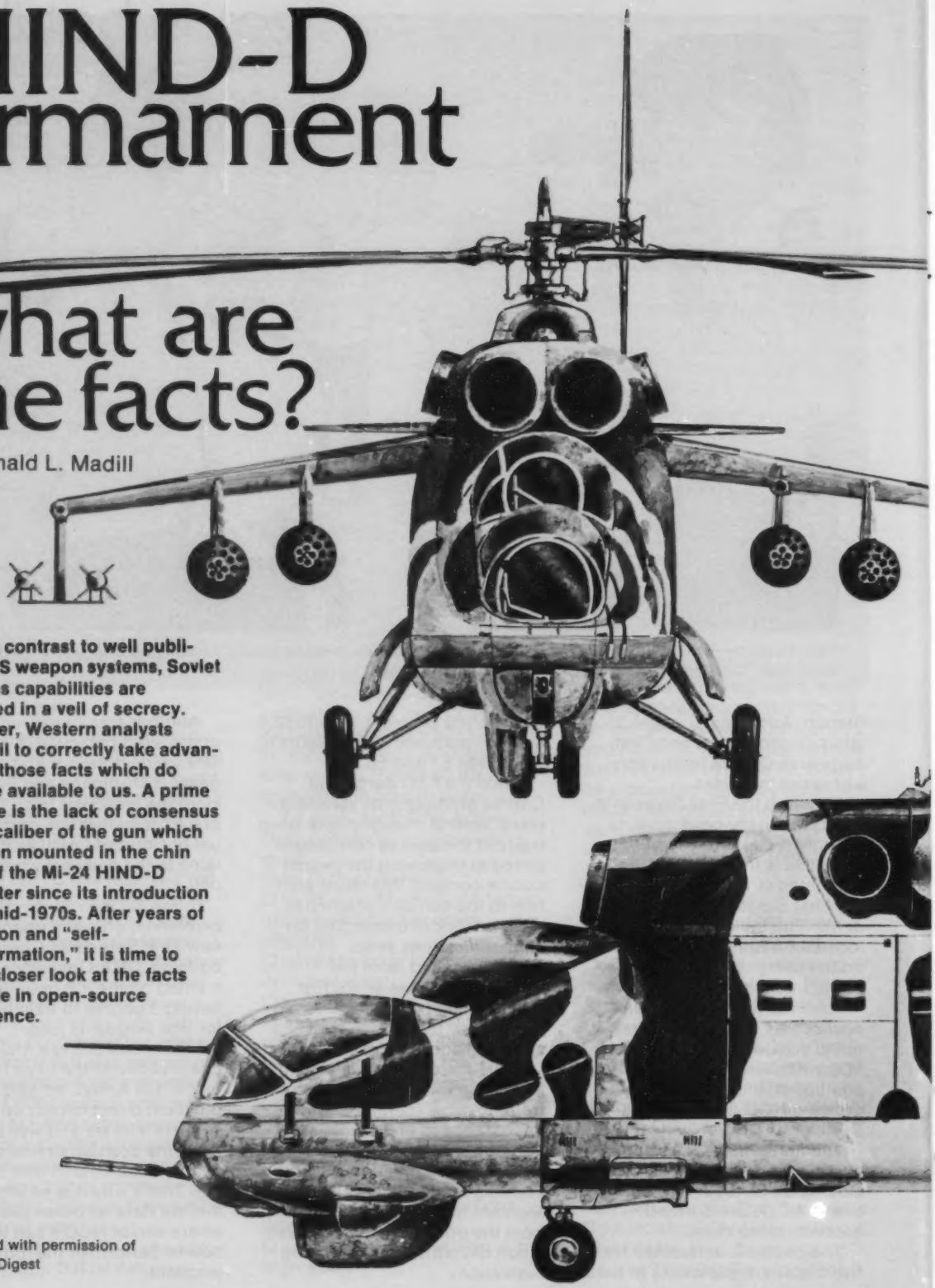
Following the ribbon cutting ceremony, officially opening the new First Sergeants Course building, SMA Connelly commented on the importance of having a course to train people for first sergeants jobs.

"The job of being a first sergeant is one of the most important in the Army," he said. "It has the most direct impact on the soldiers' morale and welfare. Also, the position of first sergeant is essential to unit training. That's why it is so important that we have a course like this where senior NCO s can learn how to perform in the job of first sergeant."

# HIND-D armament

# what are the facts?

by Donald L. Madill



**In stark contrast to well publicized US weapon systems, Soviet weapons capabilities are shrouded in a veil of secrecy. Moreover, Western analysts often fail to correctly take advantage of those facts which do become available to us. A prime example is the lack of consensus on the caliber of the gun which has been mounted in the chin turret of the Mi-24 HIND-D helicopter since its introduction in the mid-1970s. After years of confusion and "self-misinformation," it is time to take a closer look at the facts available in open-source intelligence.**

Reprinted with permission of
Aviation Digest

The Mi-24 HIND-D mounts a 12.7 millimeter (mm) four-barrel Gatling-type machinegun in its chin turret. There are no photos and no confirmed evidence for reports that this armament may be replaced by 23mm or even 30mm guns on some HINDs. Such reports appear to be based on erroneous assessments of early photos, on conjecture, or on mirror-imaging, and have lead to considerable confusion regarding the type of gun in the HIND-D turret.

The earliest open literature report of the variant which was to become known as HIND-D seems to have been published by ***Aviation Week & Space Technology*** (11 March 1976, p. 16): "Soviets have flown a new attack helicopter, with a different rotor system, tandem gunner/pilot seating, and a radar-directed 23mm gun in a chin-mounted turret." No photo of the new variant accompanied this report.

in these photographs, incorporates a turret which houses a four-barrel 'Vulcan' type 12.7mm gun." But, although the gun picture is clearly 12.7mm, the authors added, in deference to the earlier, unsubstantiated reports, "This turret can also accommodate a 23mm cannon." Other sources, such as Wiener, **The Warsaw Pact Armies** (1977, p. 380), began to report a "four-barrel 12.7mm Gatling gun," but the "23mm" seed was sown and refused to die.

Thus, articles on the HIND-D through the years have continued to represent two "schools of thought" on the gun, with about half choosing the 23mm supposition over the 12.7mm facts. The ***AW & ST*** report of "a radar-directed 23mm gun" has been repeated in such periodicals as ***Aviation Digest*** (April 1977, p. 3 and May 1978, p. 2) and ***Army*** (December 1977, p. 29), with no reference to the

(from the first mention of the HIND-D in **Jane's** supplement in ***Air Force,*** June 1977, p. 42, to the entry in the regular 1979/80 edition, p. 202) has consistently straddled the two lines of assessment by ambiguously reporting "a four-barrel Gatling-type large-calibre machinegun." Although one might assume that "large-calibre" is intended to agree with the 23mm school, it is important to note that **Jane's** also refers to the single-barrel, swivel-mounted machinegun of the HIND-A (labeled as a "12.7mm machinegun" in **Jane's** editions through 1975-76) as a "large-calibre machinegun" starting in 1977.

Rather than skirting the issue, some publications attempted to reconcile the two types of armament reported. Early on, **Armor** (March-April 1977, p. 41) followed the lead of **TC 1-88** in stating: "It is obvious that some type of Gatling gun has replaced

## the "23mm" seed was sown and refused to die

The first published photo of this "possible HIND variant" appeared in the Soviet military newspaper ***Red Star*** (11 March 1976) and was reprinted in ***Air Defense*** (October-December 1976, p. 43). The photo was of such poor quality that the "23mm" story was not disputed.

However, by March 1977, in **TC 1-88,** *Aviator's Recognition Manual,* the US Army Aviation Center at Ft. Rucker, AL, was able to publish a clear photo of the HIND-D chin turret stating correctly, "The HIND-D, as seen

12.7mm weapon confirmed in available photographs, and in ***Armor*** (March-April 1977, p. 41) was an alternative to the 12.7mm gun.

The correct assessment of the 12.7mm, meanwhile was accepted by the authors of articles in ***Armor*** (March-April 1977, p. 41), ***Flight International*** (6 August 1977, p. 418), ***Aviation Digest*** (December 1979, p. 43), and **Jane's Defence Review** (No. 2/80, p. 119).

The usually authoritative **Jane's All the World's Aircraft**

the single-barreled machinegun. The Gatling gun is probably a four-barrel, 12.7mm gun. The Soviets may elect to equip this helicopter with a 23mm cannon in lieu of the Gatling gun." This made the 23mm gun an option which might conceivably be used on some as yet unseen and unphotographed version of the HIND.

Despite the evidence of a 12.7mm weapon, the two assessments were again mixed, but with a different accent, by Turbiville in **Army** (December

**...undesirable mixtures of fact and supposition need to be eradicated before they become institutionalized.**

1977, p. 29): "This latest model has a modified nose turret which mounts a probable radar-directed multibarreled automatic weapon of unknown caliber. (The Soviet Union has at least two models of multibarreled 23mm cannon designed for use on aircraft, although it would be premature at this point to suggest that one of them has been incorporated into the Mi-24)." Nevertheless, Turbiville himself makes this "premature" suggestion on the very next page by following the **AW & ST** lead: "Armament is said to consist of a nose-mounted 23mm radar-directed gun." Thus, Turbiville planted yet another seed by suggesting that the HIND-D armament might be something like the twin-barrel 23mm GSh-23 gun carried on Soviet fighter aircraft such as MiG-21, MiG-23, and Su-24. (The six-barrel 23mm Gatling-type gun of the MiG-27 is a less likely candidate, and no aircraft is known to have a four-barrel Gatling gun.)

135), published a table which listed a "4-barrel 23mm cannon" among the armaments of the HIND-D. This has given rise to a new generation of erroneous information which has been spread by Captain McNamara in ***Military Intelligence*** (July-September 1980, p. 23) and as reprinted in ***Aviation Digest*** (January 1981, p. 47), although he also includes on the same page the correct assessment. "Latest reports indicate that it may have a radar-directed four-barrel 12.7mm Gatling-type machinegun," citing CACDA **(HB 550-2)** as his source.

The ultimate distortion, however, may be found in the normally reliable ***Flight International*** (16 August 1980, p. 612), where the author states of the HIND-D: "The 12.7mm gun of the HIND-A is replaced by a chin turret carrying a 23mm, four-barrel Gatling-type gun with a rate of fire of 3,200 rounds per minute, giving an air-to-air as well as an air-to-ground capability." The extra

by the interjection of yet another variation on the theme in **Jane's All the World's Aircraft 1979-80** (p. 202): "Other developments reported in 1979 were the introduction of some 'HINDS' of a 30mm Gatling-type nose gun and a laser seeker." The only other mention of such a weapon in connection with the HIND of which I am aware was in ***International Defense Review*** (No. 5/80, p. 682) where it is stated that the HIND-D is "likely to be supplemented soon in this close air support role by the new T-58 fixed wing aircraft. The latter seems to have been developed from the same concept as gave rise to the USAF A-10, being able to carry a heavy warload and mounting a 30mm Gatling gun. HIND-D is heavily armed and is also armoured. Chin turret mounts a four-barrel Gatling gun . . . " It is possible that a connection between the "30mm Gatling gun" reported for the T-58 ground-support aircraft and the "four-barrel Gatling gun"

**. . . air-to-air as well as an air-to-ground capability.**

More recently, the "23mm" seeds have begun to bear some strange "hybrid" fruits which could be harmful if swallowed. These undesirable mixtures of fact and supposition need to be eradicated before they become institutionalized. An authoritative source for information such as numbers of helicopters deployed but, unfortunately, not for the characteristics of helicopters, **The Military Balance 1979/80** (p. 100 or as reprinted in ***Air Force,*** December 1979, p.

detail on the rate of fire tends to lend substance to the myth/error, and the ascribed application in an air-to-air role also seems to lend credibility in light of recent attention to the possible use of the HIND in such a role. However, Captain Daschke, in ***Aviation Digest*** (December 1979, pp. 43-44) assesses the "12.7mm Gatling gun" of the HIND-D as capable of being employed in both close air support and air-to-air interdiction roles.

The picture is further muddied

(caliber unspecified) of the HIND-D has been made as the result of an error or perhaps as a conjecture that the armament of the fixed wing aircraft might also be used on the helicopter employed in the same role. The door to such an interpretation is left open by the author.

It remains to be seen whether the 30mm Gatling gun is any more of a reality than the unconfirmed reports of a 23mm gun.

# specialty proponency advocate

**This is a new column dedicated to providing information on specialty proponency matters that have a direct impact on the US Army and Military Intelligence. The following short articles outline some of the latest issues and actions your proponency agency (the US Army Intelligence Center and School) has been developing.**

## IMPLEMENTATION OF ARMY LINGUIST INITIATIVES

Long a recognized problem of the US Army, the improper use , maintenance, and low retention of enlisted linguists has become the subject of detailed meetings and briefings. Several recent proposals were designed to solve these problems. The following specific initiatives indicate where emphasis will be placed:

Increased **retention** will be through increased compensation. Compensation will be keyed to language proficiency measured by controlled testing, and will be independent of rank or duty assignment. Congressional approval, an occupational analysis to establish the inventory of required skills at each level, and development of a series of language proficiency tests will require an estimated three years before the Army can begin this initiative.

**Maintenance** will evolve through progressive language training, first at an apprentice level with advanced language training offered upon the first reenlistment. This advanced language training should prepare the linguist to assume journeyman status upon successful completion. Language training will be a combination of Defense Language Institute (DLI) courses and civilian college courses linked, if possible, to an overall goal of a bachelor degree in a foreign language.

**Use** will be improved by establishing a system of career plans. These plans will be developed by the individual and a senior counselor upon the first reenlistment. Jointly they will develop a desired sequence of assignments and training that will satisfy both the needs of the individual and the US Army. Barring drastic shifts in world events, all efforts will be maintained to keep to the coordinated sequence of linguist personnel management schedules. The US Army is also looking into how the USAF accepts, trains, and uses linguists in the implementation of desirable USAF features. In MI, establishment of a language management field (LMF) within career management fields 96 and 98 will enable the US Army to direct proponency sharing for languages with DLI and for specialty (technical skills) with USAICS. Much work remains to be done, but by the time all the new desired initiatives are fielded, the result will be beneficial to all concerned.

## AREA INTELLIGENCE SPECIALIST (97C)

Serious problems in terms of accession, retention, use, and training have been noted with respect to MOS 97C (Area Intelligence Specialist). A working action-officer meeting was recently conducted at USAICS which included attendees from INSCOM, OACSI, SSC-NCR, USAREC, and USAICS. The group consensus provided a well-coordinated design to alleviate many of the problems. The following features were agreed upon:

1. Accept applications from active-duty service personnel who have two (plus) years of active service.
2. Accept applications from prior service personnel who have served in an MI MOS for two (plus) years of active service.
3. Devise a method of selection of highly qualified 97B10 (Counterintelligence Specialist) students who voluntarily agree to alter their contract; accept language training, if applicable; and train in an area intelligence assistance training module, to be developed and taught at USAICS, Fort Huachuca, AZ.

# GEOPOLITICS

## the ultimate in key terrain

by MAJ Niel E. Nielsen

*"East-West political relations may fruitfully be considered as a long-term and inalienable struggle between the insular* ***imperium*** *of the United States and the 'Heartland'* ***imperium*** *of the Soviet Union."* Colin Gray

**The Geopolitics of the Nuclear Era**

Historians, political scientists, economists, and strategic-military analysts agree that geography is an important factor in evaluating the actual or potential military power of an adversary. The following rhetorical question will guide us in a brief overview of geopolitics: Do geographical characteristics such as location, size and shape, natural resources, and population density predetermine a nation's political and military density?

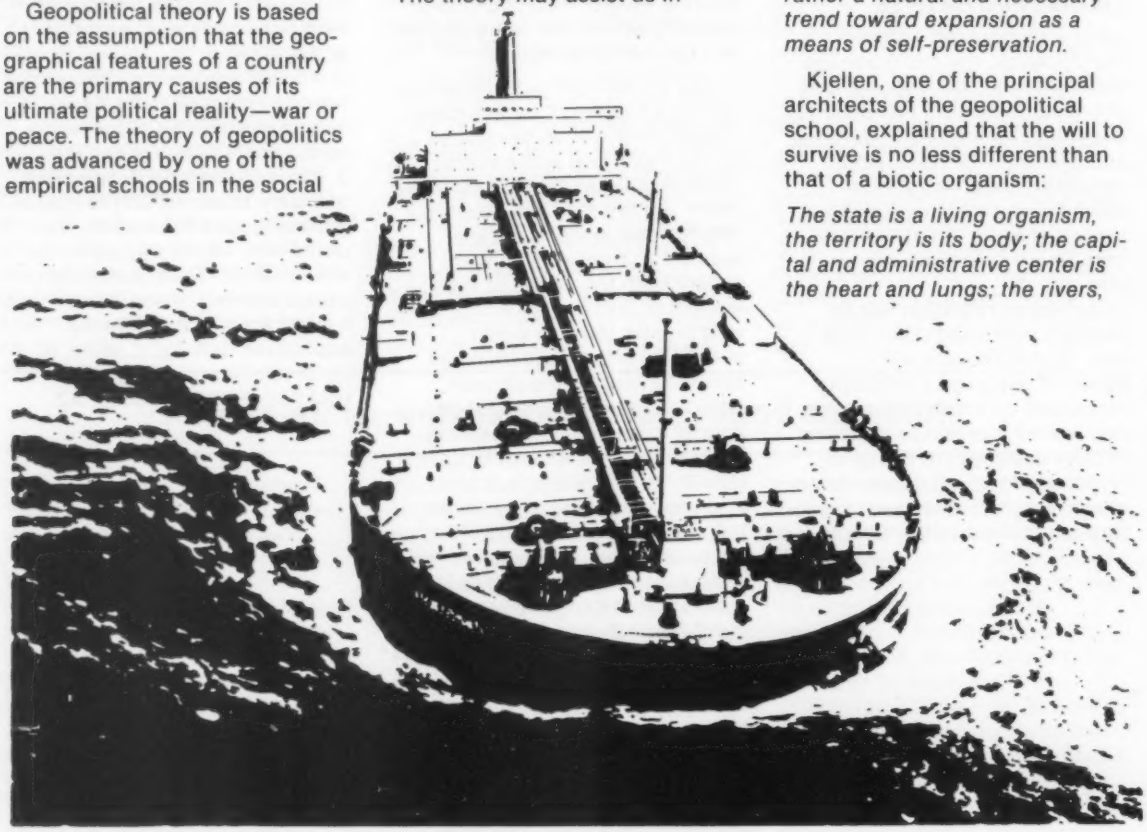
Geopolitical theory is based on the assumption that the geographical features of a country are the primary causes of its ultimate political reality—war or peace. The theory of geopolitics was advanced by one of the empirical schools in the social era of determinism which was fashionable at the turn of the 20th Century. The heading geopolitical proponents (Ratzel, List, Haushofer, MacKinder, and Kjellen) declared that a nation, like a biological organism, must by every available means secure the essential for its continued natural growth and ultimate survival. This theory, if true, has profound ramifications affecting the delicate international balance of power between the free world, the Soviet bloc, and the emerging third-world countries. The theory may assist us in attempting to understand the interwoven struggles and tensions which have characterized the twentieth century. Geopolitics may still have a residual benefit in portraying and predicting the short-, intermediate-, and long-term objectives of our allies, and adversaries' national interest.

Geopolitical theorists such as Ratzel and Kjellen assert that a nation must expand economically and militarily to survive. Ratzel explains:

*Vitally strong states with a limited area of sovereignty are dominated by the categorical political imperative to enlarge their area by colonization, union with other states, or conquest of different types . . . It is not the raw instinct of conquest but rather a natural and necessary trend toward expansion as a means of self-preservation.*

Kjellen, one of the principal architects of the geopolitical school, explained that the will to survive is no less different than that of a biotic organism:

*The state is a living organism, the territory is its body; the capital and administrative center is the heart and lungs; the rivers,*



*roads and railroad are arteries and veins; and the areas with raw material are food necessary for growth of the limbs.*

This metaphorical analogy may help us understand the strategic overview and intentions of the worldwide communist expansion since World War II. Communist doctrine, when translated into "real world" military parlance, states the military conquest of a neighbor's natural resources may be the only alternative open to a state, which would allow it to continue its growth and survival; the stronger of the two states must, for its own national self-sufficiency, capture and dominate its neighbors' territory and natural resources.

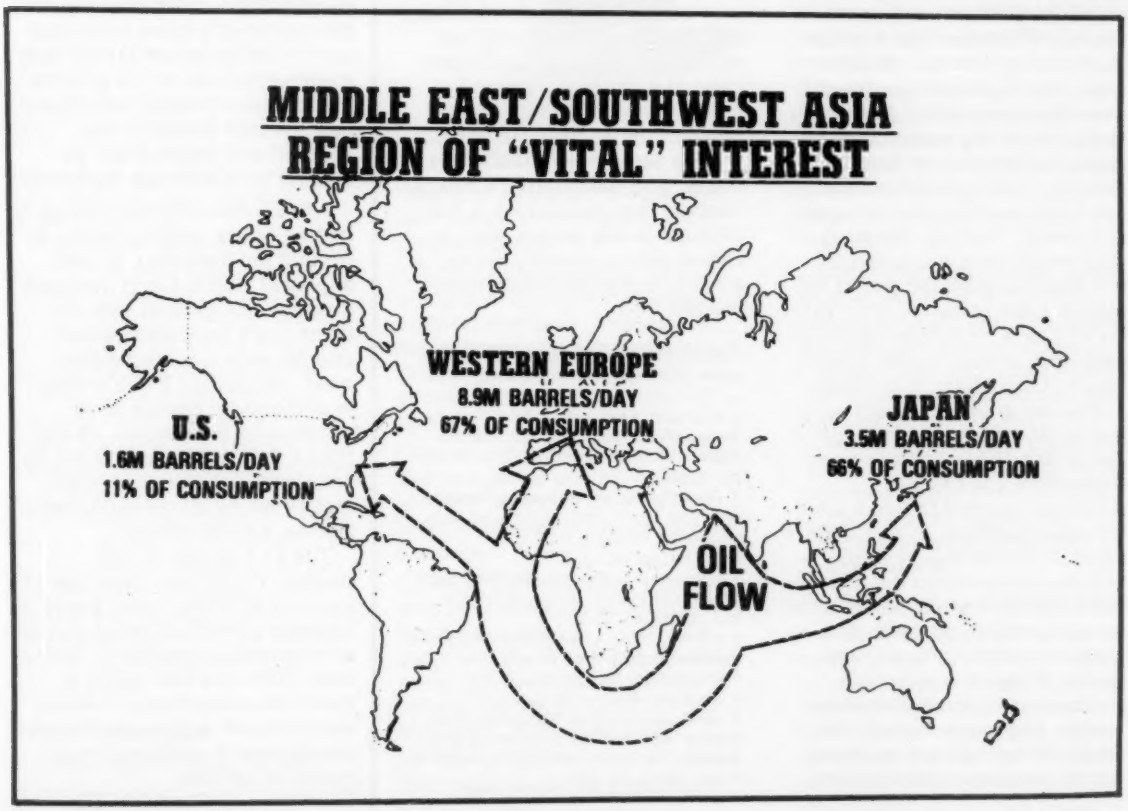
The bases of geopolitical theory are space and position. According to Ratzel, "These two [space and position] determine the geographical value and ultimate destiny of every part of the earth's surface." The political and military development of a nation is caused not by accidental political or historical consequences, but by its natural resources, size and shape, raw materials, and population. Thus, geography, not its people, determines the political reality; this is the premise of geopolitics.

The basic geographical characteristics of the nation-state—its location, size and shape, climate, population density, and natural resources—were viewed by geopoliticians as the parameters for growth and survival.

The major military powers of World Wars I and II were the USSR, France, England, Italy, Germany, and the United States. Except for the United States, which was geographically isolated, each country suffered the ravages of war. The location of a country in terms of its relationship to land and oceans predetermines its primary military offensive and defensive posture. Strategic location is as essential for maintaining peace as it is for waging war.

Size and shape is the second criterion used to evaluate the actual or potential military and economic strength of a nation. The geopoliticians identified two distinct types of size and shape: attenuated (for example, Norway, Chile, and Sweden); and great inner depth (for example, the USSR, United States, and China). Because of their size and shape, these latter nations are relatively easier than elongated nations to defend from attack.[5]

Next in the geopolitical formula is climate.[6] The geopoliticians declare that all powerful states are located between the middle latitudes, and the majority of the world's developing nations are located in the lower latitudes. Adverse climatic conditions directly affect a nation's progress and military presence. Certain regions of the earth, by



their nature, are too wet, too cold, too hot, or too dry to establish and maintain a large standing military force. For example, the Antarctic region, the Arctic Circle, and the Amazon lowlands have little military value in contrast to the Strait of Hormuz, the Strait of Gibraltar, or the Suez Canal.

The fourth component of geopolitical theory is population density. Overpopulated nations may be forced to wage war on their neighbors so that extra territory can be taken and colonized to relieve the pressures of their overpopulation.

Japan, in the Russo-Japanese War of 1904-05 and again in World War II, attacked larger countries in the expectation that ultimate victory would give them the additional territory, or living space, to grow and expand in.[7] China, with her immense population, seeks such a "living space." Since the Treaty of Nerchinsk in 1689, which fixed the boundary between the Russian and Manchu powers, the Chinese and Russians have fought over the Amur Valley. According to Kjellen, living space (Lebensraum) predetermines political density. Thus, Lebensraum is a key factor in the power struggle of a nation. Perhaps the struggles which have characterized the blood-soaked regions of the Middle East, known as the "Valley of Tears" in the last two mideast wars, exemplify the importance of this factor to a nation.

The last geopolitical criterion is natural resources.[8] In the jargon of the 1980s, "oil becomes the bottom line natural resource" needed to fuel a country's war machine. In World Wars I and II, the German military complex understood the necessity of acquiring additional natural resources to become, and sustain itself as, a world superpower. Today the petroleum products from the Middle East (which must pass through the Strait of Hormuz) are as important to the free world and communist bloc countries as aluminum, zinc, rubber, and copper were to the Central Powers (Austria, Hungary, and Germany) in World War I and the Axis Powers (Germany, Japan, and Italy) in World War II.

The theory of geopolitics is not offered as "the" panacea in understanding the complex military realities of today's or, even more importantly, tomorrow's changing conditions. No one theory can accurately explain or predict a nation's military intentions. However, when the theory of geopolitics is used with other methods of analysis (socioeconomic or political), it may serve to identify, clarify, and forecast the intentions, motives, and national interest objectives of our adversaries. The theory of geopolitics was popular and accepted at the turn of the century. It was later rejected and replaced by other conventional theories; however, the theory may be useful in understanding the struggles for regional and worldwide dominance. Specifically, the location, size and shape, climate, and oil-soaked lands of the Middle East including the Strait of Hormuz, Suez Canal, and the Strait of Gibraltar reaffirm that geopolitics is the ultimate in key terrain. Key terrain is not necessarily the top of a hill—it's the land underneath the hill.

1. Rudolf Kjellen, **Der Staat als Lebensraum** (Berlin: Berlin-Grunewald, 1924), p. 75.
2. Russel H. Field and G. Etzel Pearcy, **Geopolitics in Principle and Practice** (New York: Ginn and Company, 1944), pp. 10-15.
3. Friedrich Ratzel, **Politische Geographie** (3rd Ed.: R. Oldenbourg, Munich and Berlin, 1923), p. 239.
4. Ratzel, op. cit., p. 250
5. Norman J. G. Pounds, **Political Geography** (New York: McGraw-Hill Co., Inc., 1963), pp. 51-2
6. Lucile Carlson, **Geography and World Politics** (Englewood Cliffs, N. J.: Prentice-Hall, Inc., 1938), pp. 76-7.
7. Field and Pearcy, op. cit., pp. 35-7
8. Johannes Mattern, **Geopolitik Doctrine of National Self Sufficiency and Empire** (Baltimore, Md.: Johns Hopkins Press, 1942) pp. 109-11.

## AAFES tightens check cashing

After Oct. 24, the Army and Air Force Exchange Service (AAFES) will tighten its policy on cashing nonpersonalized checks. "Nonpersonalized checks may be cashed up to a maximum of $50.00 and checks accepted in payment for merchandise will be limited to $250.00," said an AAFES official.

According to AAFES policy, a personalized check must have the customer's name imprinted on it. Customers who trade with local banks that do not provide personalized checks, and those patrons able to verify their account and balance will be exempt from this new restriction.

AAFES directed this change to its free check cashing policy to protect the customer. A 1980 survey of CONUS and overseas installations showed that five times more nonpersonalized checks were returned dishonored. "More than $16.5 million in dishonored checks were received by exchanges. Of that figure, $1.3 million could not be collected, and that loss is ultimately felt by all our customers," said an AAFES official.

The $1.3 million in lost revenue could have been used to improve services, lower prices or increase contributions to morale and recreation programs. Therefore, cashing a bad check is much like shoplifting. In effect, we are stealing from each other because each consumer must make up the loss.

# mohawks in hostile airspace

by CPT William C. Weaver

Maximum friendly support is essential when committing an aircraft to a Photo or IR mission. (SLAR is normally flown behind friendly lines.) Missions flown around 1st echelon forces are exposed to a high degree of enemy hostility.

Timely and accurate information concerning known and suspected enemy air defense sites is important for preflight planning. Information from the corps all-source intelligence center (ASIC) is integrated with the aerial surveillance unit's preflight briefings to provide the most accurate description of the hostile airspace.

It is essential in preflight planning to determine the priority of threat targets, critical node targeting, other service's intelligence, and current updates. Unit intelligence support will insure that the crew has the latest information.

## Friendly Support

Coordination must be complete and continuous throughout the planning and execution stages of a mission. Respective elements will interface at each command level:

☐Artillery coordination takes place at division or corps fire support elements. Requests for fire suppression and fire support coordination measures will be provided through fire support plans.

☐Air escort is requested through the tactical air control center (TACC), and may only be practical for operations in controlled airspace.

☐TACC interface occurs daily so that the aerial surveillance unit can be included in the air task order (ATO). This is the major point of coordination the day before a mission, since Army aircraft fly in Air Force controlled airspace.

☐Air defense artillery (ADA) coordination first occurs at corps. Division ADA plans are used in mission planning to increase the opportunity for counterair suppression. Specific air corridors may be established and be available for OV-1D missions.

☐Electronic warfare (EW) support can take many forms. Airborne jammers are coordinated at the TACC. Army assets would be tasked through the G3 for targeting specific weapons systems.

☐Communication coordination is reflected in the ATO. Additional call-signs and frequencies are provided through corps interface with subordinate units. Call-signs and frequencies are established for reporting, and contacting forward air controllers (FACs) and front line units. Inflight reporting to front line units is done using call-signs and frequencies provided in the Recce request.

## Flight Planning Coordination

A daily aerial reconnaissance/surveillance (DARS) conference is conducted at corps headquarters. Normally, the conference is held in the morning with representatives from corps, division, and the TACC. At the meeting, information on aircraft availabil-

ity is provided (normally by a liaison officer from the aerial exploitation battalion or AEB), and the sortie rate for the next 24 hours is established based on the expected battle plans, preplanned mission requests, and unit support priorities, considerations are also given to manpower levels, aircraft availability, and crew rest states.

The 24-hour period is divided into "blocks" of four or six hours. Sorties are assigned to a specific time-block for a supported command's use. The allocations identify preplanned and immediate (ground alert) sorties.

Following the meeting, the corps G-2 Recon and Surveillance (R&S) representative coordinates with the direct air support center (DASC) and the TACC representatives to insure that the required sorties for tomorrow's operations are included in the Air Force ATO. This document is written by the TACC current plans section listing the total air operations expected for the next 24 hours in Air Force controlled air space. The ATO provides the AEB with necessary flight plan information for the next day's missions. If target areas are not specified at the coordination meeting, the ATO shows the mission as a ground alert sortie. Strong justification must exist to fly Photo/IR missions around 1st echelon areas, and targets must be defined before takeoff.

The AEB operations section receives the ATO, double checks the information previously provided to the CISE, and confirms the status of each mission request. During the surveillance and reconnaissance validation process, the aerial surveillance (AS) company and the EW company are alerted. The imagery interpreters assigned to the AS company prepare maps and define target coverage.

The EW company's operations section reconfirms its tasking with AEB operations and also notifies its own communication-electronics (C-E) platoon, maintenance platoon, and aerial platoon. An operations management center at the flight line helps disseminate critical mission-tasking information. The unit's flight crew normally reports to the AS company's imagery interpreters two hours before takeoff and confirms target coordinates, flight routes, imagery requirements, threat update, and friendly support.

The flight crew works with the image interpreter to thoroughly plan the mission. Every crew procedure and mission situation will vary; however, some basic considerations are as follows:

1. Situation:
   a) Enemy locations—known and suspected.
   b) Enemy air defense weapons systems locations.
   c) Suspected enemy intentions.
   d) Friendly situation.
2. Mission:
   a) Sensor(s).
   b) Target(s), method of coverage, and coordinates.
3. Execution:
   a) Sensor employment.
   b) Routes.
   c) Time over target (TOT), time enroute, and mission duration.
   d) Reports—when, where, and how information recorded.
   e) Altitudes.
   f) Coordination with support elements.
4. Administration and Logistics:
   a) Termination airfield.
   b) Special equipment requirements.
   c) Emergency procedures.
   d) Debriefing procedure.
5. Command and Signal:
   a) Air-ground communications/frequencies, call signs, and secure monitoring.
   b) Modes/codes.
   c) Communications/Electronics Operations Instructions (CEOI).
   d) Units to receive in-flight reports.

The crew takes advantage of previously flown missions and the opportunity to use sources of information from other AEB collection assets to create the most accurate threat picture in the mission area.

### Conduct of the Flight

The mission must conform to the ATO. All previously planned support is keyed to the aircraft executing the meticulously planned mission. The OV-1D aircraft is the key player—the center of attention. Any deviation from the original plan of action must be reported up the chain of command to corps and laterally to each support element. Planning has been continual up to this point for both preplanned and immediate missions. Time has been budgeted properly, each element has done its job, and the crew is left to orchestrate the mission to its conclusion.

During aircraft runup, all systems are checked for mission employment. Failure of a system (or any malfunction) will require immediate analysis and a decision of whether or not to continue. It may become necessary to provide backup aircraft for sensitive missions. The pilot and aerial sensor specialists work as a team. Radio calls are arranged for in advance and all cockpit responsibilities are defined before takeoff.

Following takeoff, sensors are activated and reports are made to Air Force radar control facilities in accordance with the ATO. If the mission requires penetration of enemy first-echelon weapons systems, the aircraft proceeds through the battle area, descending in altitude to low-level flight. Once below Air Force controlled airspace, normally 500 feet, the aircraft should check with friendly ground units if coordination was made for passage through their airspace. Coordination with Air Defense units increases the chance of safe passage.

Before descending below 500 feet, a check with the Air Force control facility determines the

availability of an airborne or ground FAC at the entrance to the mission area. The FAC provides a point of coordination and a source of timely information about the enemy's activity, and other aircraft using Army airspace below 500 feet. At low altitudes, the use of aircraft radios is extremely limited, unless communications are made with other aircraft at higher altitudes.

During visual/photo missions, in-flight data is recorded throughout. Reports are made via secure means when practical. In-flight reports to the requesting unit will largely determine the success or failure of the mission.

Conceivably an aircraft can visually observe the target and report in-flight; at that point in time the mission has been successful. Additional information of intelligence value may be collected, noted, and later reported during the flight. If the aircraft is outside the range of enemy first-echelon weapons systems, a more routine report is practical. For SLAR, the information passed via data link to the ground sensor terminal is the major source of information for the supported unit. Hard-copy imagery isn't normally provided; information passed electronically to the requestor is the fastest means of dissemination. Currently a Reconnaissance Exploitation Report (RECCEXREP) is prepared within 30 minutes of landing.

Once the aircraft has entered first-echelon force areas (friendly and enemy), they will be exposed for 3 to 5 minutes in the area. There won't be time to renegotiate for artillery support, EW jammers, or Air Force fire suppression. The crew will be committed to the mission and left to their aircraft survivability equipment if friendly support fails.

Returning from a SLAR mission is done according to the ATO or inflight instructions received from the control and reporting center (CRC). When returning from a target area through uncontrolled airspace, friendly unit coordination becomes paramount. Again, FAC coordination increases the exchange of information and mission flight paths. Higher altitudes are possible as the aircraft proceeds toward the friendly rear area. Once into controlled airspace, contact is established with the Air Force radar facilities for the flight to home base.

### Completed Mission

It is essential that imagery interpreters debrief the crew immediately following the mission. The entire flight path is retraced, and all information is

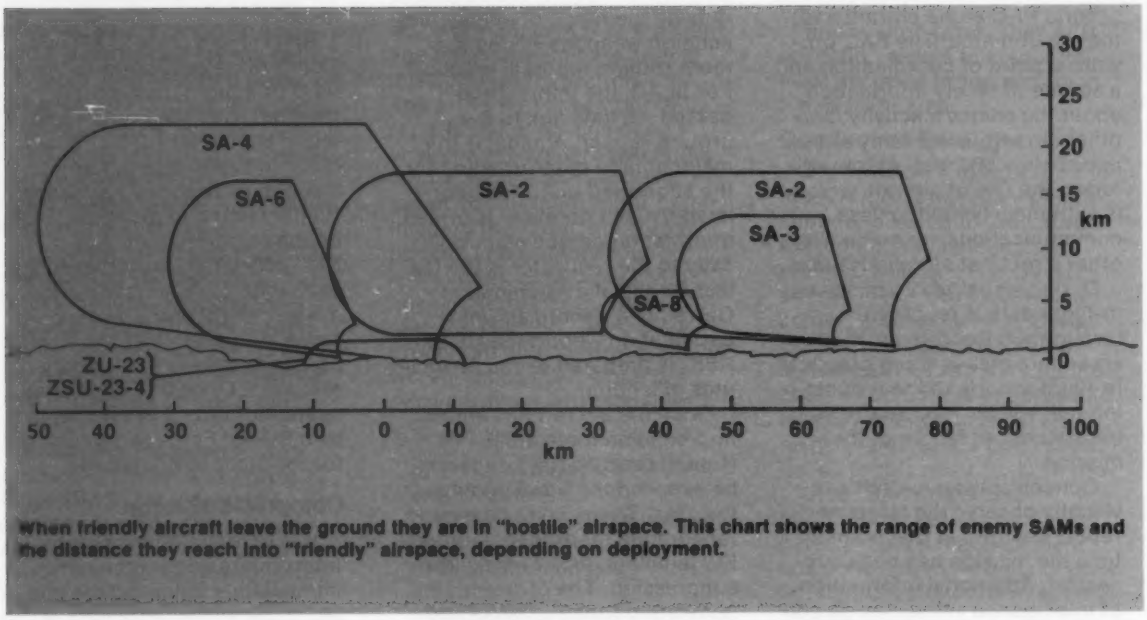
# coming in the next issue:

**Conducting a SIGINT/EW ARTEP** by Captain Jeffery A. Sorenson

**Cuba in Angola: A Balance Sheet** by Captain Tom Adams

**Ethics in Intelligence** by Lieutenant Colonel William G. Hanne

The theme for the next issue is Tactical Intelligence. Articles will cover all fields of intelligence support to the tactical commander. Any tactical intelligence article will be considered for the next issue if it arrives before March 1, 1982. All article submissions are welcome at any time.




**When friendly aircraft leave the ground they are in "hostile" airspace. This chart shows the range of enemy SAMs and the distance they reach into "friendly" airspace, depending on deployment.**

recorded for correlation with other intelligence.

The imagery is processed and evaluated to insure proper target coverage and response to the commander's essential elements of information (EEI). Other information may become available as required imagery interpretation reports are formed and disseminated.

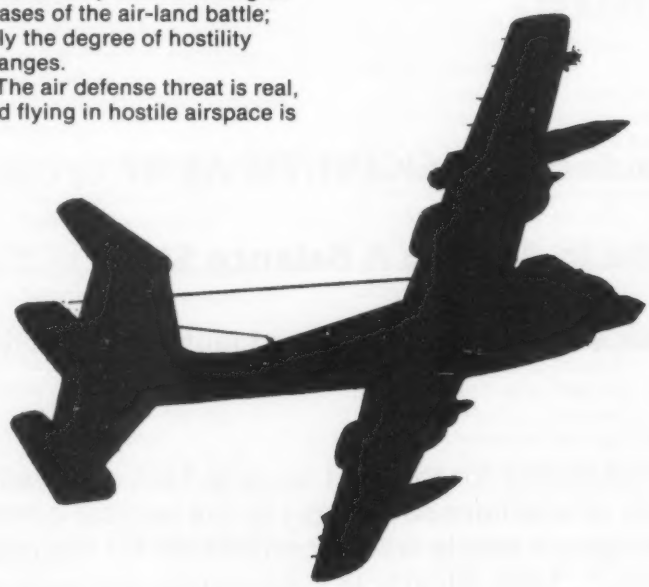
A successful mission provides the necessary information for correlating and producing timely intelligence.

**Conclusion**

This special discussion covers many ideal situations presented for the best employment of a sensor asset. Realistically, SLAR missions will take priority over all other OV-1D mission requests. Photo and IR mission requests will be judged on their individual merits and will consider the availability of support. The mechanics of coordinating the support of all assets is extremely difficult. The probability of the desired support being available for a single OV-1D mission in the most hostile areas on the battlefield will always be situational dependent. EW compounds the coordination efforts, requiring contingencies for each phase of a mission. Survivability will constantly be evaluated by asset managers as each commitment is met.

There is no pure "standoff" or "penetration" mission. As soon as the aircraft leaves an airfield, it is picked up by enemy collection systems. The airspace is continuously hostile during all phases of the air-land battle; only the degree of hostility changes.

The air defense threat is real, and flying in hostile airspace is dangerous. To increase the survivability of the aircraft and crew, a great deal of friendly support is required. By coordinating this support and insuring its timeliness, an aircraft can complete its mission and survive to fly again.



# SECURITY EDUCATION IN USAREUR

by SFC Gary Arrasmith and SSG David Rash

A primary mission of a peacetime army is training. For any type of training to be effective, it must be both meaningful and interesting. The United States Army, Europe (USAREUR) is striving to meet this goal in its security education program.

Implementing meaningful and interesting security education programs poses a challenge to Army security-managers worldwide. Frequently, higher headquarters tell their subordinates, "You've got to develop a viable security education program." And that's all they do—tell someone else to do it. Unit-level security managers seldom receive tangible assistance, and don't have the expertise or assets with which to start meaningful and interesting programs. Each level of higher headquarters must play a vital role in stimulating the thought processes. We can, and must, provide the food-for-thought that will give unit security managers the hors d'oeuvres to whet the security education appetite of their commands. This article provides the reader a menu used by USAREUR.

To assist units in developing necessary programs, HQ USAREUR provides the latest security-related information through a variety of media. The most frequently used is the *Newsbulletin for Information and Personnel Security* (NIPS), which is published monthly.

Along with most other major commands (MACOMs), HQ USAREUR provides the "what" in new policy via electrical message and the "why" via NIPS. This reduces the burden on an already overtaxed message system. The NIPS is a tool used to pass working plans originating in USAREUR to its other MACOMs.

Through NIPS solicitation, input was obtained from the field and was instrumental in activating the once-dormant USAREUR security-poster series. Though our poster program isn't where we want it, it's on the move. USAREUR currently has 21 different posters in stock and has a target of 45 to 50 posters by July 1982. Our ultimate goal of 208 posters envisions each unit displaying four posters a week in key locations, with a new set each week. The USAREUR poster program emphasizes quality and effectiveness, not just the number available. The use of subtle humor and new, eye-catching themes has contributed greatly to the program's success.

Besides regulatory requirements, the posters also focus on the hostile intelligence threat.

In USAREUR, we are geographically eyeball-to-eyeball with our potential adversaries, and their hostile intelligence activities are numerous and resourceful. Therefore, Subversion and Espionage Directed Against the Army (SAEDA) is of prime concern to commanders and security managers. Attending classes, however, is often tedious for the soldier.

On the other hand, when tasked to teach the class, how often have you wanted to present a SAEDA/threat briefing, but lacked dynamic, relatively current examples—the ingredients so badly needed to keep the presentation from being bland. HQ USAREUR provides the ingredients with a SAEDA/Security Education Assistance Letter (a quarterly command letter which disseminates the latest SAEDA-related information available). Dealing primarily with current examples of hostile intelligence services' approach techniques, the letter provides education specifically tailored for USAREUR. Eliminating or sanitizing SAEDA reports, in coordination with the Office of Deputy Chief of Staff for Intelligence (ODCSI CI) counterintelligence experts, allows us to present meaningful and interesting unclassified data, which is necessary because the majority of USAREUR's soldiers and civilians don't have security clearances.

Another frequently used medium is the USAREUR Security Managers' Seminar. These seminars are presented by Information and Personnel Security Specialists from ODCSI, HQ USAREUR. They allow those who actually do the work in the field to talk directly with the nebulous "they" of that faraway headquarters. This one-on-one contact provides an invaluable exchange between policy and practical application, and an opportunity for exchanging security education/training ideas on an informal basis. The specialists from ODCSI open the seminar with a 30- to 45-minute pitch explaining new policy and its rationale, and covering problem areas observed from the headquarters level. The remainder of the time is devoted to a question-and-answer period and an exchange of ideas.

**In USAREUR, we are geographically eyeball-to-eyeball with our potential adversaries, and their hostile intelligence activities are numerous and resourceful.**

During the past year, HQ USAREUR presented over 20 seminars to 900 service members from 430 units. The seminars are held at key locations throughout Germany based on the troop population's center of mass. This insures that no unit has more than 1-hour's

travel time and keeps our TDY costs to a minimum. Understandably DA MACOMs, which have units located hundreds of miles apart, may not find it feasible to provide their resident specialists for such seminars. However, using the MACOM's major subordinate units to perform this interface aspect of security education should not be overlooked.

The media described above are not necessarily new or totally innovative. However, when combined with two USAREUR-unique programs, security education approaches the degree of utility and effectiveness that USAREUR subordinate units have the right to expect—and certainly deserve.

**. . . those who actually do the work in the field . . . talk directly with the nebulous "they" of that faraway headquarters.**

The first USAREUR-unique program is the training course for security managers presented by the 7th Army Training Command (7th ATC). Over 3,100 USAREUR students have completed this course since its creation in 1977, and is the only one of its kind in the United States Army. Designed with a multifaceted approach, the course touches upon each area in the field of security to include information, personnel, operations, and physical security. The course provides selected officers, warrant officers, noncommissioned officers (E-7 and above), and DA civilians (GS-7 and above) with the basic information needed to perform their duties with emphasis on "how" to perform those duties and the "why" of governing policy. Selection is not based on MOS, but on assignment and projected assignments to security-manager duties.

Although not designed exclusively for security education, the 7th ATC also presents a 3-week Tactical Intelligence Course with a curriculum geared toward the combat intelligence specialist. An important aspect of this course is that the entire first week of instruction is dedicated to the same information presented in the security managers' training course. Through this program of instruction, 7th ATC has insured that personnel attending either course will receive the same security education, and that these students will become tomorrow's educators throughout the command.

The second USAREUR-unique security education program is provided by the Armed Forces Radio and Television Service (AFRTS), Europe. Through the Command Information Support the Armed Forces Network (AFN) uses 15-second radio and television spots to pass security-related information to USAREUR members and their dependents. With these locally produced commercials, AFN uses security education messages provided by HQ AFRTS. Both formats provide high visibility in the AFN for security education.

We are the first to admit our good fortune in having this media to spread the word, and we realize that the majority of commands don't have this service at their disposal. However, with the ever-increasing popularity and availability of video recording and closed-circuit television for Army training purposes, the opportunity to interject a security message during normal training, or to develop professional productions for dissemination throughout a post or Army MACOM, is a definite reality.

**...paper does not protect paper;... People protect paper!**

With the August 1979 edition of AR 380-5, USAREUR elected to eliminate continuous administrative accountability (CAA) for the vast majority of SECRET documents throughout the command. Our rationale for eliminating CAA was that paper does not protect paper; a DA Form 3964 by itself will not prevent loss, theft, or compromise. People protect paper! That's where security education must be continuous, effective, and a part of the day-to-day business of the security manager. Security managers are in both the security and the education business because each person handling classified material is a vital, basic element in every security program.

At HQ USAREUR, we are well aware that our current security education program is not all-inclusive. However, it is a firm foundation on which to build. With the continuous evaluation of feedback from USAREUR units (and, we hope, from the readers of this article), we are finding that it is possible to make security education both meaningful and interesting without taxing the subordinate units.

# no-notice intelligence 82d style

by Captain John F.O'Shaughnessy, Jr.

**A character from Kurt Vonnegut's novel *Slaughterhouse Five*, once said, "Some day there's going to be a knock at your door." The statement accurately explains the need for the 82d Airborne Division to remain constantly poised for immediate deployment.**

The intelligence community supports the mission of the 82nd. This is a tall order, particularly considering that "immediate deployment" means wheels up on the first aircraft within 18 hours of notification. This tactical aspect of the division's mission makes it imperative that the intelligence agencies understand the 82nd's special requirements and can tailor the collection effort when necessary.

Now , however, intelligence agencies outside the tactical units are not programed to meet the time limits imposed upon the 82nd Airborne Division, nor should they be. The requirement of tactical units to extract valuable intelligence from strategic resources adds to the problem of providing commanders on the ground with recommendations.

Each brigade in the 82nd has a section that is ideally suited to support airborne commanders—the Battlefield Information Coordination Center (BICC) (see diagram). A properly trained section has the capability to store, analyze, and disseminate tactical intelligence which requires a different perspective and must be extracted from strategic collection assets.

The success of any tactical mission requires intelligence on the enemy, weather, and terrain. In this respect, an airborne division is no different from any other division. However, the 82nd requires more detailed information on the enemy's size, equipment, and weapons to determine the exact mix of assets that will fill the limited aircraft available. More airframes are required to counter an armor threat than a lightly armed force. The airborne tactics employed and the rules of engagement are also developed from intelligence and analysis.

Weather prediction is such a vital factor for airborne operations that detailed statistics must be prepared monthly for all "watchcon" related areas. Weather conditions with only a hampering effect on other units can abort an airborne operation or significantly lower the chances of success. For instance, high winds disperse drop patterns and increase jump injuries. Low visibility hampers locating the drop zone. Illumination affects assembly time and movement, a vital ingredient of success. Finally, the temperature range affects the amount of equipment necessary, and this impacts on the amount of ammunition that can be carried due to weight restrictions. For example, a 150 lb. paratrooper boarding an aircraft for winter operations, even without live ammunition, can weigh 300 lbs. or more.

The most important data required for airborne operations is knowledge of the terrain. Success is dependent on the ability to assess the enemy's intentions and capabilities, and to determine how terrain will force him to configure to accomplish his mission. Terrain information guides the planning sequence of an airborne operation from its inception. Photos of drop zones and tactical objectives are vital. Sandtables constructed from these aids guide paratroopers for quick assembly into a fighting force after being dropped over a large area. Terrain features affecting enemy mobility must be analyzed to enable specific weapons systems to be optimally employed.

The results of recent division deployments indicate the necessity for, and the past lack of, responsive intelligence. In the fall of 1980, the division was alerted to send a battalion-size force to Fort Indiantown Gap, Penn., on a civil disturbance mission. Although it is an operational military reservation, no maps were available for planning and little was disclosed about the refugee camp layout or its occupants. During the 1978 Zaire alert, the division commander was briefed from a world atlas. The large scale was quite useless for planning airborne operations. Finally, a recent G2 of the 82nd was a rifle company commander during the Dominican Republic deployment in 1965. He landed without the benefit of a map.

Accurate, current intelligence is required to support the strategic mission of the airborne, and the data base must be comprehensive and easily disseminated. Only the national level assets have the capability and flexibility to collect the data required and are doing so now. The disconnect now revolves around the dissemination phase. The 82nd moves too quickly for intelligence to flow down or requests for information to be answered. Consequently, the 82nd needs to have an organic ability to develop, analyze, and store information pertinent to probable deployment areas. That capability is present within the BICC. It is essential that we develop an information base on areas targeted for possible deployment. As a tactical unit responsible for the conduct of strategic missions, the 82nd needs to bridge the gap between the division and the national level assets that provide direct support. The BICC, through information provided from outside sources, can develop a target packet on "hot spots" that will give the commander a head start in the 18-hour sequence. Further intelligence disseminated upon receipt of the mission can be integrated into a final intelligence estimate.

To optimize the use of an analysis section at brigade level, a continuous, comprehensive training program is required. The 96B in the BICC must be comfortable performing terrain analysis, order of battle development, assessment of military capabilities, and the integration of diverse data into an accurate and concise intelligence estimate. He must also be familiar with both organic and supporting intelligence collection systems, a necessity considering the likelihood of an airborne brigade being separately deployed and requiring support from high-level assets. The BICC must be both a finely tuned tactical

machine in the field and a continuous collection and analysis center in order to prepare for the no notice alert.

The training of these soldiers must have a high priority. Programs that have enhanced and sharpened the skills of the intelligence analysts in the 82nd's 1st Brigade include:

**1. A BICC FTX.** Tactical Operations Center (TOC) functions in the field isolating the S2 section through control cell inputs and simulating coordination with other sections, subordinate, adjacent, and higher units. (This is also a great time for a refresher on common skills.)

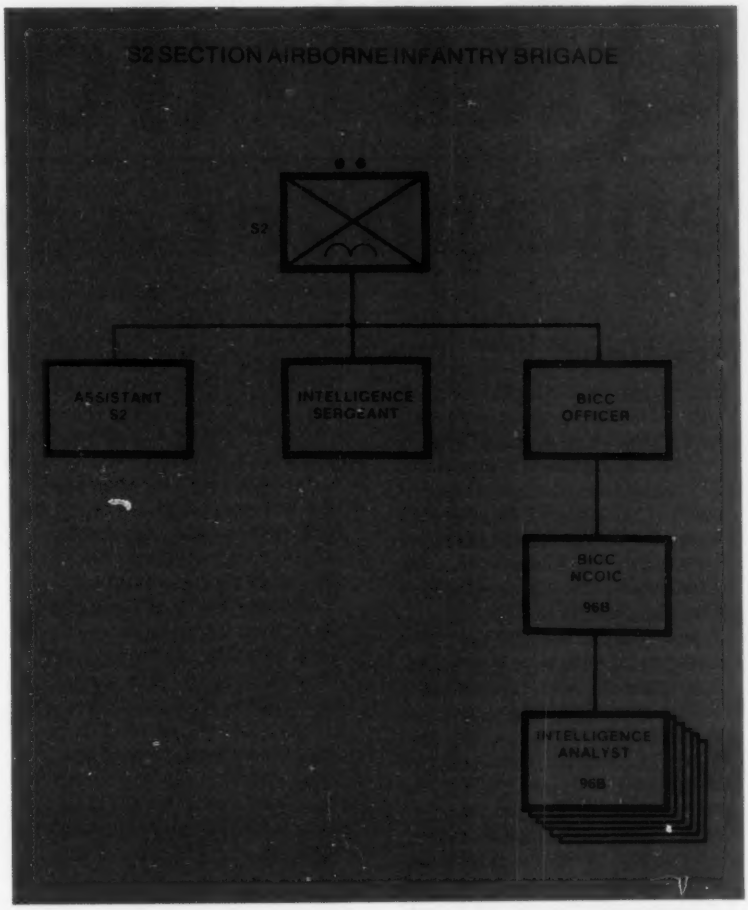
**2. Classes.** Subjects from IPB and collection planning to OPFOR capabilities and limitations (classified whenever possible).

**3. Development of target folders.** From a company raid intel packet to a full staff contingency study on a possible deployment mission gives the analyst an opportunity to employ the intelligence cycle to create a final product using imagery, terrain data, and OPFOR tactics.

**4. Development of real world intelligence estimates.** A brigade size drop in Florida, a battalion off-post exercise to Utah, Panama, or Alaska are common occurrences that provide ideal opportunities to train the entire unit. Also, unfamiliar surroundings, an unknown, illustrates the necessity for plans and orders to be based on actual intelligence.

**5. Scenario development.** FTX'S, ARTEPS, and CPXS allow the analyst to use his knowledge of the OPFOR to provide a realistic background to an operation. Even more of a challenge is to ensure the OPFOR players present a valid picture of the enemy.

**6. Exporting intelligence awareness.** Each soldier in the BICC presents classes to units within the brigade serving a dual function: one, training in presenting classes teaches briefing techniques and instills self-confidence; two, the line units are given unclassified information on OPFOR capabilities and deployment possibilities. Information absorbed prior to an alert will be invaluable once the paratrooper hits the ground. As an example, in a recent "Ivan Week" presented in the 1st Battalion Airborne, 504th Infantry, the brigade BICC provided classes on "The Soviet Airborne" and a "World Hotspots Briefing."




By providing 96B's with additional expertise, while insuring the basics are not neglected, a professional, effective intelligence section is entirely possible. Three brigade BICCS within the Division provide an interface between units. This is necessary as the Division rotates mission responsibilities between brigades. Data and studies from the national level would not be closeted away in one brigade but would benefit all.

The airborne BICC is an answer to the dilemma of providing intelligence support to units with no-notice deployment requirements. It can provide accurate intelligence estimates with information collected prior to an alert along with information integrated after notification. The BICC also provides a focal point for coordinating the collection and analysis effort for the brigade after it deploys through coordination with organic and higher level intelligence assets. The BICC provides the airborne infantry the intelligence they require. Who is more suited to the task than a fellow paratrooper, a companion in combat?

# QRT*-dora:

# epitaph for a spy

by Col. Richard S. Friedman

## Reminiscence

During the second week of August 1981, there appeared in the **International Herald Tribune** an item from a brief Hungarian MTI press release announcing the death of Sandor Rado in Budapest. Other newspapers in Europe and North America also noted briefly the passing of Professor Doctor Sandor Rado, Doctor of Science, Doctor of Economics, Fellow of the Royal Geographical Society, and co-president of the Hungarian Society of Geodesy and Cartography. Few of the obituaries alluded to Professor Rado's unusual role as a principal in a major intelligence drama of the Second World War. As Defense Attache to the American Embassy in Budapest, from 1977 to 1980, I had the opportunity to meet Sandor Rado. He was "Dora," the codename assigned to him by the Soviets, by which he operated throughout his wartime clandestine career.

I remember the last time I conversed with Rado, during the final year of his life. It was on the 14th of July, in the garden of the residence of the French Ambassador in Budapest at the traditional Bastille Day reception. There was Sandor Rado, in his usual good humor, resembling a "Kewpie doll." He was wearing a dark suit with a number of decorations in his lapel, radiating charm and vitality as he exchanged jokes and observations with other international guests.

*QRT is the international radio communication signal: "Closing station - no further transmission."

In my last conversation with Rado, I told him I wished to say farewell because I was being transferred from Budapest. I thanked him for sharing with me some of his reminiscences and vast knowledge of ancient maps. Rado wished me luck in the future, as we chatted briefly. Before parting, I asked him, "Professor Rado, will we ever know the complete story of the **Dora** network, and what happened to you in Russia after 1945? What about your ten years in the Lubjanka prison? That seems a strange reward for someone who did so much for the Soviet war effort." Rado pursed his lips and folded his hands across his generous paunch. Jovially, with his bright eyes twinkling, he responded: "I wrote a book **(Dora Jelenti** "Dora Codename"); others have written books also; these books tell of many things. It is enough for everyone to know that I worked in a common cause with all those who were fighting against Hitler—all of the published accounts agree on this, if nothing else. It is my hope that I will be remembered mainly for my contributions to geographical science."

Sandor Rado made some significant contributions to the study of geography and cartography; however, it is most likely that his activities as **Dora,** the spy, will secure his name in history. His work affected the lives and fortunes of many during a critical period in world history. Now, with his passing, it seems less likely that the whole story of Dora will appear.

## Early Years

Sandor Rado was born in 1899 in Budapest into a comfortable bourgeois family. The young Rado received an excellent classical education which was interrupted by the outbreak of the First World War. He was mobilized at the age of 17 into the Austro-Hungarian Army in which he served as a junior staff officer in the Artillery. Because he was stationed in Budapest, Rado was able to continue his university education. It was during the ferment of the later, postwar years that Rado became a communist.

After the collapse of the Central Powers and the signing of the 1918 Armistice, there was a Social Democratic republic in Hungary, headed by Count Karolyi. The Hungarian Republic of Karolyi lasted for less than a year, but was then overthrown by a communist revolt headed by Bela Kun in which Rado joined the Red Army as a political officer. When this revolution collapsed, after 133 days, Rado had to flee for his life to Austria where he studied geography at the University of Vienna. Rado's Vienna years were busy ones. He had to work to support himself, but managed to find time to study and engage in numerous political activities. In 1921, he was sufficiently well known in communist circles to be selected for travel to Moscow to attend the Third International.

In 1922, Rado moved to Berlin for advanced scientific studies, and also to court a young Berliner whom he had met while she had been working in Vienna.

Within the following year, Sandor Rado married Helene Jansen. The young couple moved to Leipzig where Rado finished his studies and published the first geographic atlas of the USSR, a venture which established him quickly as a recognized cartographic authority. This early success was interrupted after Hitler came to power, and, in the late Spring of 1933, the Rado family moved to France. For the next two years, Sandor Rado continued his geographic research. In researching and revising his work on the **Soviet World Atlas,** Rado had to travel to Moscow in 1935. It was during this trip that he was recruited to work for Soviet Army Intelligence by S.P. Ourisky, its director.

## Espionage Activities

In 1936, Rado (codenamed "Dora") was sent to Brussels, but was unable to operate from there. He and his wife and children moved to Geneva, Switzerland, where Rado was successful in establishing himself in the map publishing business.

During 1936 and 1937, Rado was very busy as he ran his commercial business, continued his scientific research, and expanded his clandestine intelligence collection. Any one of these activities would have been sufficient to fully occupy most average men. But Sandor Rado was not an average man.

In April 1938, his Soviet control, who operated out of Paris, informed him that, effective immediately, the Paris residency was to be closed. Sandor Rado was to become the resident director in Switzerland for Soviet intelligence and, henceforth, would report directly to the Intelligence Center in Moscow. The Russian turned over all of his Swiss network to Rado.

Until the summer of 1939, Rado busied himself developing and expanding his agent network. He was able to provide useful information on German preparations for the occupation of Danzig and other related military and political events. Once war broke out, however, Rado needed to acquire a radio communications capability, previously unnecessary. Rado's search for communications and information soon put him in contact with Alexander Allan Foote, who was established in Switzerland as an expatriate Briton. Foote, who was to become Rado's assistant, was involved with British Intelligence and with the Soviets. Rado soon acquired a radio transmitter and operator. Almost immediately a regular and considerable flow of intelligence was being sent to Moscow. There appears to have been some continuing competition between Rado and Allan Foote for control of Soviet intelligence activity in Switzerland which later caused problems for both of them. The first published account of their wartime operations was in Foote's book, **Handbook for Spies,** printed in 1949. This book, which was on every Fort Holabird Officer's recommended reading list for many years, provided a highly selective history of intelligence activities in Switzerland directed against the Axis between 1940 and 1945. For a long time, it was the only open source of information on this subject. German records, captured after the war, revealed relatively little. The Swiss revealed nothing publicly for many years. Rado, himself, disappeared from view in 1945 and did not surface again for ten years.

It is well known that Rado (Dora) provided Moscow with a volume of high-quality intelligence almost from the moment he commenced operations. What is less well known, however, is that Dora's reports were rejected at the top level because they failed to conform to existing beliefs. On 17 June 1941, Dora transmitted the following message to Moscow:

> 17.6.1941 For Director
> About 100 infantry divisions are now positioned on German-Soviet border. One-third are motorized. At least ten of the remaining divisions are armored. German troops are concentrated in Romania at Galatz, and elite, special-mission divisions have been mobilized. The 5th and 10th divisions stationed in German occupied Poland are taking part. Dora.

At Moscow Center, the information from Dora was assessed as accurate because similar or identical information was provided from other sources. Unfortunately for the Soviets, Josef Stalin and his entourage did not believe any of it; they felt they had a clear and positive insight into German plans, and so the initial objectives of Hitler's **Operation Barbarossa** for the invasion of the Soviet Union were achieved. Those who had correctly reported the intelligence did not fare well—several lost their lives, and many lost their freedom. Rado, however, being in place in Switzerland, not only continued to operate but achieved a new credibility with his masters for the accuracy of information produced by his network.

The counterintelligence and security authorities of Switzerland were primarily concerned in World War II with protecting Switzerland against hostile activities. Intelligence gathering inside Switzerland which did not violate Swiss laws, provoke undue attention, produce violence, or otherwise give the Swiss some cause for apprehension apparently was noted, sometimes casually, but little interference resulted. German counterintelligence, on the other hand, as a result of investigative successes in Belgium, was able to unravel a considerable part of the Moscow-run networks, and, from 1942, knew about Rado and his communications system.

Through early 1943, the Dora network continued to function with mixed results. Rado was under continuous pressure because Moscow nagged him to equal or repeat his past successes. Finally, in April 1943, Dora was able to provide the

Moscow Center with vital information concerning the Kursk salient. Today, historians are in general agreement that the battle for Kursk was the decisive turning point in the war. A German victory, while unlikely, was still possible before Kursk. After the Russian victory at Kursk, German defeat was thereafter certain.

## Decline of Dora

When the Germans attacked Kursk on 5 July, in **Operation Citadelle,** General Rokossovsky and his Soviet forces, because of Dora's information, were able to anticipate German moves. By the beginning of August, the Kursk battle was finished, and the Soviets took to the offensive. After Kursk the Dora network never again achieved the volume or quality of production that had characterized their performance since Rado began to operate in 1939/40. On the contrary, the overall situation for Dora seemed to deteriorate as individual agents were picked up, codes were compromised, and sources seemed to become less productive. In October it became obvious to Rado that he was in personal danger because the Swiss authorities had become more actively interested in him, and he was forced to go into hiding. Not long after this time, his British associate, Foote, was arrested and briefly jailed by the Swiss. Rado was able to make his way to Paris where he contacted the Russians, informing them that the Dora network was finished in Switzerland.

Then, Foote also arrived in Paris and reported to the Soviet mission. Foote's account of the operations of the **Dora** network differed from that supplied by Rado. Faced with the inconsistent reports, in early 1945, both Foote and Rado were ordered to report to Moscow. Because the war was still active in Europe, their aircraft was routed through Marseilles and Cairo. During a stopover in Cairo, Rado disappeared into the Egyptian countryside. Later, in the summer of 1945, Rado, hiding in Cairo, was apprehended by the British. Because he had been travelling on a Soviet passport, he was turned over to the Soviets and flown immediately to Moscow, where he was quickly consigned to Lubjanka prison until 1955. During a post-Stalin amnesty, Rado was permitted to return to Hungary for the first time since his departure in 1919. His wife Lene soon joined him, and, following a lengthy illness, she died in 1958. Lene was buried beneath an imposing monument in Budapest which attested to her lifelong dedication and service to communism and her wartime activities.

## The ULTRA Connection

A number of theories have been advanced since the early 1950's concerning Rado's operations and the end of the Dora network. An excellent and detailed history, **Operation Lucy,** published in 1980 by Anthony Read and David Fisher, advances the theory that Foote had been employed by British Intelligence together with Rudolf Rossler (codenamed Lucy) to use Rado and his network as a conduit to pass highly secret and sensitive ULTRA materials to the Russians without revealing or compromising this extraordinary source. (ULTRA was the code for intelligence obtained through Allied signal intelligence intercepts and cryptanalysis during World War II.) Foote, in his **Handbook for Spies,** did not propose any particular theory, but depicted Rado as a hard-working, occasionally inept spendthrift. Rado, by his own admissions, in 1945, was unable to account for all of the operational funds entrusted to him, and it is possible he diverted some of the money to his own use. It is a historical fact that Rado violated some of the basic principles of covert operations. As a result, some of his agents were apprehended, and some of his communications were compromised.

Gilles Perrault, author of **The Red Orchestra,** described the operations of Rado's network and the Red Orchestra (the Soviet network operated in Germany, France, and Belgium) under the direction of Leopold Trepper as having been the victims of internecine intelligence strife during the Stalin era because they had been managed by Soviet Military Intelligence Chief, General Berzin. Berzin was eliminated by Stalin early in the War, and a widely accepted theory was that anyone involved with Berzin automatically became suspect by Stalin.

Some of the information passed by Dora to Moscow Center could have come from ULTRA sources. In some instances it is difficult to reach any other conclusion. It is clear that after the Kursk Offensive, Dora never again received very much quality intelligence from his various sources. Anthony Read and David Fisher **(Operation Lucy)** present an extremely persuasive argument for the ULTRA theory by pointing out that, after the horrendous Wehrmacht defeat at Kursk, the British no longer felt they had to risk ULTRA secrets by channelling them through the Dora network because by that time normal UK-Soviet liaison channels had been established, thereby making it unnecessary in any event.

## Leopold Trepper

Some insight into Rado's attempt to avoid returning to Moscow developed in 1975, upon the publication in France of **The Red Orchestra,** the memoirs of Leopold Trepper. Trepper was the redoubtable director of the Soviet Military Intelligence network which operated in Belgium, France, and Germany during World War II. Rado and Trepper were passengers on the same aircraft in 1945, en route to Moscow at the time Rado disappeared. Trepper observed: "While we were flying toward Moscow, Rado's disappearance (in Cairo) obsessed me. I knew he had performed his mission beyond all expectation, that he had nothing to reproach himself for.... In Switzerland, he had contributed substantially to



☆ U.S. GOVERNMENT PRINTING OFFICE: 1981—783-058

the victory, but because of his profound understanding of the facts, his realism as a man of learning, he felt in spite of victory, nothing had changed in the kingdom of the OGPU (KGB). He foresaw the fate that awaited him in Moscow. He did not care for the prospect of ending his life in one of Stalin's jails; hence he disappeared in Cairo after making sure his wife and children were safe in Paris." Trepper, himself, was not so fortunate. As he related: "The Truth Rado perceived did not strike me with its blinding light until later. I was too naive." Trepper paid for his naivete with more than ten years in prison in Lubjanka and Lefortovo, during which period he was continuously interrogated and accused of unspecified "crimes against the Soviet Union."

Finally, in the post-Stalin "thaw" that occasioned the release of Rado and others, Trepper was permitted to return to Poland where he became a virtual prisoner until 1973, when, following intense Western pressures, he was permitted to emigrate to England, and later to France. Rado had by then returned to Budapest.

Perhaps Trepper's commentaries can provide some possible insight into the thoughts and motivation of his contemporary, Professor Rado. In the epilogue to his book, **The Great Game,** Trepper says:

> "I do not regret the commitment of my youth. I do not regret the paths I have taken. In Denmark, in the Fall of 1973, a young man asked me in a public meeting: 'Haven't you sacrificed your life for nothing?' I replied, 'No'. No, on one condition; that people understand the lessons of my life as a communist and a revolutionary, and do not turn themselves over to a deified party. I know that youth will succeed where we have failed, that socialism will triumph, and that it will not have the colour of the Russian tanks that crushed Prague."

## Postscript

Allan Foote died in 1956; **Lucy** (Rudolf Rossler) died in 1958; and Lt. Colonel Sir Claude Dansey, KCMG, who had set up and managed the British Intelligence operations in Switzerland, died in June 1947. With the recent death of Sandor Rado, the most knowledgeable principals are unavailable to enlighten historians.

It appears today that the theories about Rado and his operations could be wholly correct, partially correct, or false; it is likely we may never know. But this lack of certainty probably no longer makes much difference, because the intended result—the defeat of Hitler—was achieved. The little pear-shaped professor apparently secured a place for himself in history. His status is not as he would have preferred, as a cartographer and geographer dedicated to the advancement of geodesic science, but rather as an individual caught up in the history of his time, involved in an epic struggle between great powers—as a spy!

In Western tradition, there are Valhallas for the fallen warrior; for example, the cavalryman has Fiddlers' Green, and the sailor has his Davy Jones' locker. I suspect Professor Sandor Rado might yet be radiating charm and telling jokes in six languages in some special place for old spies, whose name and location, of course, cannot be revealed. QRT/DORA

**feedback continued from page 3**

Baerman on **Intelligence Training for Maneuver Units,** but I wish he had gone a bit further with his idea on an intelligence training kit.

All the other articles were equally well done. After reading the articles on officer and enlisted career management, I must remark that it appears someone has finally figured out what went wrong during past wars and has taken steps to correct some of the problems. It is most unfortunate that this system was not implemented several years back.

It will also be another milestone when the "Intelligence professionals" receive the same treatment as other professionals—a separate promotion list. I have seen numerous MI Lieutenants simply look at the system, decide early that there was no way they could compete with other officers, and simply left the system.

When you consider that most of our wars have been fought by large bodies of relatively untrained people, there is no reason to suspect that future wars will be any different. At present our National Guard Units have no MI slots; as a result any Lieutenant who wants to remain as an MI officer rapidly figures out that he has no future in the system and rapidly leaves, and we are always back to square one.

I hope all these thoughts may be of some value to you — again keep up the good work. This issue was outstanding.

**William L. Howard**
Major, Armor USAR

US Army Intelligence Center and School
Military Intelligence Magazine
ATTN: ATSI-TD-LPM
Fort Huachuca, AZ 85613

Penalty for Private Use: $300

2DC203108005
THE ARMY LIBRARY (ANRAL-TS)
ATTN: ACQUISITIONS SECTION
ROOM 1A518, PENTAGON
WASHINGTON, D.C. 20310
01

MILITARY INTELLIGENCE.
OCT 1981
V.7 I.4 C.1

*B$ 4$ -$*